Produkthandbuch
Revision A

McAfee Quarantine Manager 7.1.0

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

MARKEN

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee und das McAfee-Logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource und VirusScan sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

LIZENZINFORMATIONEN

LIZENZVEREINBARUNG

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWARE-PAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSEITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN McAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **7**
Informationen zu diesem Handbuch 7
Zielgruppe 7
Konventionen 7
Quellen für Produktinformationen 8

1 Einführung **9**
Verwalten von Quarantäne und Spam 9
Lieferumfang der MQM-Software 10

2 Bereitstellungsszenarios **11**
Verwenden von MQM mit unterstützten McAfee-Produkten 11
Hochverfügbarkeit 12
Richtlinienverwaltung 12
VMware-Unterstützung 13

Installation

3 Installation **17**
Voraussetzungen 17
Übersicht über die Installationsschritte 18
Vorbereiten der Installationsumgebung 19
Konfigurieren der Microsoft SQL Server-Datenbank 19
Installieren von MySQL for McAfee Quarantine Manager 19
Konfigurieren von MySQL 5.1 für Linux oder Microsoft Windows 20
Installieren von McAfee Quarantine Manager 21
Installieren von McAfee Quarantine Manager in einer Cluster-Umgebung 21
Konfigurieren eines Clusters unter Windows 2003 Server 21
Konfigurieren eines Clusters unter Windows 2008 oder 2008 R2 Server 22
Deinstallieren von McAfee Quarantine Manager und Komponenten 23
Deinstallieren der McAfee Quarantine Manager-Software 23
Deinstallieren von MySQL for McAfee Quarantine Manager 23
Upgrade auf die aktuelle Version von MQM 23

4 Integrieren von McAfee Quarantine Manager in ePolicy Orchestrator **25**
Vorbereitungsschritte für die Integration 25
Bereitstellen des McAfee Quarantine Manager-Pakets und der Erweiterungen 26
Installieren von MQM auf dem McAfee ePO-Server 26
Bereitstellen von McAfee Agent auf Client-Computern 26
Einchecken des McAfee Quarantine Manager-Pakets 27
Einchecken des Pakets „MySQL for McAfee Quarantine Manager“ 27
Bereitstellen der Komponente MySQL for McAfee Quarantine Manager 28
Bereitstellen von MQM auf Client-Computern 29
Installieren der McAfee Quarantine Manager-Richtlinienerweiterung 30
Installieren der McAfee Quarantine Manager-Berichtserweiterung 30

Installieren der MQM-Hilfeerweiterung . . . 31
Festlegen von Richtlinien in ePolicy Orchestrator . . . 31
Erstellen und Bearbeiten von Richtlinien . . . 32
Erzwingen von Richtlinien . . . 32
Senden eines Aufrufs zur Agentenreaktivierung zum Abrufen neuer Eigenschaften bzw. Richtlinien . . . 33
Konfigurieren von Berichten . . . 33
Deinstallieren von McAfee Quarantine Manager mit ePolicy Orchestrator . . . 34
Entfernen von MQM von Client-Computern . . . 35
Entfernen der Pakete . . . 35
Entfernen der Erweiterungen . . . 36

5 Arbeitsschritte nach der Installation 37
Konfigurieren der Datenbank . . . 37
Testen der Installation . . . 38
Erneutes Branding von McAfee Quarantine Manager . . . 39

Konfiguration und Verwendung

6 Server-Verwaltung 43
Administratortypen . . . 43
Authentifizierungsmodi . . . 44
Verwenden von LDAP-Gruppen als McAfee Quarantine Manager-Administratoren . . . 44
Erstellen von Administratoren mit eingeschränkten Berechtigungen . . . 45

7 Domänenverwaltung 47
Hinzufügen oder Importieren von Domänen zu McAfee Quarantine Manager . . . 47
Hinzufügen von Domänen . . . 48
Gleichzeitiges Importieren mehrerer Domänen . . . 48
Exportieren von Domänen . . . 48
Zuweisen von Domänen zu Domänenadministratoren . . . 49
Ändern von Domänenkonfigurationen . . . 49
Ändern mehrerer Domänenkonfigurationen . . . 50
Erstellen einer Zuordnung zwischen Domänen und Gruppen in verbundenen McAfee-Produkten . . . 51

8 Verwalten von Benutzerkonten 53
Erstellen von Benutzerkonten . . . 53
Importieren von Benutzern über LDAP . . . 53
Importieren von Benutzern anhand einer CSV- oder TXT-Datei . . . 54
Importieren von Benutzern anhand einer XML-Datei . . . 55
Automatisches Registrieren von Benutzern . . . 56
Ändern der Benutzerkonfiguration . . . 57
Registrieren einer Verteilerliste . . . 57

9 Verwalten isolierter Elemente 59
Suchen nach isolierten Elementen . . . 59
Durchführen von Aktionen für isolierte Elemente . . . 59

10 Verwalten von Tasks 61
Konfigurieren einer geplanten Digest-E-Mail . . . 61
Konfigurieren geplanter Datenbankbereinigungen . . . 62
Automatisches Synchronisieren und Registrieren von Benutzerlisten . . . 62
Automatisches Senden von Statusberichten . . . 63
Synchronisieren von Verteilerlisten . . . 63

11 Übermittlungen durch Benutzer 65
Verwalten der Übermittlungen durch Benutzer . . . 65
Anzeigen von Suchergebnissen . . . 66

12 Benutzerinteraktionen 67
Anmelden bei McAfee Quarantine Manager . . . 67
Verwalten von isolierten E-Mails über die Benutzeroberfläche . . . 68
Verwalten von isolierten E-Mails über Digest-E-Mails . . . 70
Übermitteln von Spam-Proben an McAfee Labs . . . 70
Übermitteln von auf einem Datenträger gespeicherten Spam-Proben . . . 71
Übermitteln von Spam-Proben mit dem Customer Submission Tool von McAfee . . . 71
Übermitteln einer Probe eines fälschlicherweise isolierten Elements . . . 72
Verwalten Ihres McAfee Quarantine Manager-Kontos . . . 72
Verwalten der Blacklist . . . 73
Verwalten der Whitelist . . . 73
Ändern des Kennworts . . . 74
Konfigurieren der Voreinstellungen für den Quarantäne-Bericht . . . 74
Verwalten von Aliassen . . . 75
Anzeigen von E-Mail-Neuzuweisungen . . . 75

Pflege und Berichterstellung

13 Server-Wartung 79
Verwalten der Server-Konfigurationen . . . 79
Anzeigen von Protokolleinträgen . . . 79
Konfigurieren der Protokolleinstellungen . . . 80
Konfigurieren der Kommunikation zwischen MQM und anderen Produkten . . . 81
Konfigurieren der erweiterten Server-Einstellungen . . . 82
Konfigurieren von Zertifikaten für die sichere SMTP-Kommunikation . . . 86
Sichern der Datenbank . . . 86
Sichern der Microsoft SQL Server-Datenbank . . . 87
Wiederherstellen der Microsoft SQL Server-Datenbank . . . 88
Sichern der MySQL-Datenbank . . . 88
Wiederherstellen der MySQL-Datenbank . . . 88
Konfigurieren eines geplanten Sicherungs-Tasks für die MySQL-Datenbank . . . 89

14 Verwaltung von Blacklists und Whitelists 91
Blacklist- und Whitelist-Ebenen . . . 91
Konfigurieren des Konfigurationsübertragungsintervalls . . . 92
Verwalten von Blacklists und Whitelists . . . 92
Importieren von Blacklists und Whitelists . . . 93
Exportieren von Blacklists und Whitelists . . . 94

15 Dashboard und grafische Berichte 95
Anzeigen von Dashboard-Zählern . . . 95
Testen von verbundenen McAfee-Produkten . . . 95
Durchführen einer Schnellsuche . . . 96
Berechnen der Datenbankgröße . . . 96
Erstellen von mehrdimensionalen Berichten . . . 96
Erstellen von Top-10-Berichten . . . 97
Erstellen von spezifischen grafischen Berichten . . . 97
Herunterladen eines Berichts . . . 98

A Häufig gestellte Fragen 99

B Erneutes Branding von McAfee Quarantine Manager 105

Übersicht 105

Anpassen der McAfee Quarantine Manager-Software an das Erscheinungsbild Ihres Unternehmens 105

Hinzufügen des eigenen Logos 105

Verwenden der Unternehmensfarben 106

Ändern des Firmen- und Produktnamens 106

Änderungen an der Darstellung der Oberfläche für Benutzer 106

Index 107

Einleitung

In diesem Handbuch finden Sie die erforderlichen Informationen für die Arbeit mit Ihrem McAfee-Produkt.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation wurde von McAfee nach eingehender Recherche mit Blick auf die Zielgruppe verfasst.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren**: Personen, die für die Implementierung und Durchsetzung des Sicherheitsprogramms eines Unternehmens verantwortlich sind.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.
	Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.
	Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

Nach der Veröffentlichung eines Produkts werden Informationen zu dem Produkt im Online-Knowledge Center von McAfee eingegeben.

Vorgehensweise

1. Rufen Sie im McAfee ServicePortal unter http://support.mcafee.com die Registerkarte **Knowledge Center** auf.
2. Klicken Sie im Bereich **Knowledge Base** auf eine Inhaltsquelle:
   - **Produktdokumentation** für die Suche nach Benutzerdokumentation
   - **Technische Artikel** für die Suche nach KnowledgeBase-Artikeln
3. Wählen Sie **Meine Filter nicht löschen** aus.
4. Geben Sie ein Produkt ein, und wählen Sie die Version aus. Klicken Sie dann auf **Suchen**, um eine Liste der gewünschten Dokumente anzuzeigen.

1 Einführung

McAfee® Quarantine Manager (MQM) fasst die Funktionen der Quarantäne- und Anti-Spam-Verwaltung mehrerer McAfee-Produkte zusammen.

Die Software bietet einen zentralen Ausgangspunkt für die Analyse und Behandlung isolierter E-Mails und Dateien. Diese Elemente werden isoliert, weil sie als Spam, Phishing, Viren, potenziell unerwünschte Programme oder sonstige unerwünschte Inhalte erkannt wurden.

Die Integration in McAfee® ePolicy Orchestrator® (McAfee ePO™) ermöglicht zentrales Richtlinien-Management und grafische Berichte.

Inhalt

- *Verwalten von Quarantäne und Spam*
- *Lieferumfang der MQM-Software*

Verwalten von Quarantäne und Spam

McAfee Quarantine Manager ermöglicht es Administratoren und Benutzern, ihre Anti-Spam-Produkte kontinuierlich zu optimieren und die Effektivität der Spam-Filter zu erhöhen.

In McAfee Quarantine Manager können Sie Folgendes durchführen:

- Erstellen von Administratorkonten zum Verwalten von Daten für bestimmte Domänen.
- Verwalten und Konfigurieren von Einstellungen mit der ePolicy Orchestrator-Verwaltungs-Software per Remote-Zugriff.
- Anmeldung bei McAfee Quarantine Manager mit Anmeldeinformationen von Active Directory oder Lotus Domino, Novell eDirectory, Sun System Directory oder Open LDAP v3.
- Pflegen des McAfee Quarantine Manager-Kontos: Erstellen von Administratoren, Zuweisen von Administratoren, Übermitteln von Elementen an Warteschlangen, Generieren von Berichten und Neuzuweisen von Administratoren.
- Verwalten von Blacklists und Whitelists für Benutzer, globalen Blacklists und Whitelists sowie Blacklists und Whitelists für Gruppen.
- Automatisches Synchronisieren von Benutzern und Verteilerlisten zwischen mehreren LDAP-Servern wie Active Directory, Lotus Domino, Novell eDirectory, Sun System Directory und Open LDAP v3.
- Verwalten von isolierten Elementen wie Spam-Mails, Phishing-Mails oder anderen potenziell schädlichen Elementen.
- Speichern von isolierten Elementen mit MySQL 5.1, MySQL on Linux, Microsoft SQL 2005, Microsoft SQL 2008 oder Microsoft SQL 2012.
- Durchführen von Quarantäne-bezogenen Aufgaben, beispielsweise die Freigabe von Nachrichten oder das Übermitteln von Beispieldaten an McAfee Labs.

- Verwalten von Protokollierung, Debug-Verfolgung und Melden von Fehlern an McAfee.
- Anzeigen von Digests zu isolierten Nachrichten.
- Neuzuweisen von isolierten Elementen eines Benutzers zu einem anderen Benutzer.
- Freigeben von E-Mails, die fälschlicherweise als Spam, Phishing, unerwünschter Inhalt oder potenziell unerwünschtes Programm isoliert wurden.
- Benutzer können eigene Blacklists und Whitelists erstellen und ändern; zudem können sie alle isolierten Nachrichten freigeben oder löschen, indem sie auf den entsprechenden Link im E-Mail-Digest klicken, den Benutzer von McAfee Quarantine Manager empfangen.

Lieferumfang der MQM-Software

McAfee stellt MQM als Archivdatei zur Verfügung, die von der McAfee-Website heruntergeladen werden kann.

Wenn Sie die MQM-Software von McAfee erhalten haben, sind unabhängig von der Art der Verteilung dieselben Installationsschritte erforderlich.

MQM umfasst folgende Komponenten, die zusammen oder getrennt installiert werden können:

- MQM
- MySQL for MQM
- MQM-Paket für McAfee ePO mit Richtlinien, Berichten und der Hilfe

2 Bereitstellungsszenarios

Hier werden die einzelnen Bereitstellungsszenarios ausführlich mit Diagrammen und Informationen erläutert, um Ihnen die Vorbereitung der Bereitstellungsschritte zu erleichtern.

Inhalt

- *Verwenden von MQM mit unterstützten McAfee-Produkten*
- *Hochverfügbarkeit*
- *Richtlinienverwaltung*
- *VMware-Unterstützung*

Verwenden von MQM mit unterstützten McAfee-Produkten

MQM bietet Quarantäne-Verwaltungsdienste für McAfee® Email Gateway, McAfee® Security for Microsoft Exchange (MSME) und McAfee® Security for Lotus Domino.

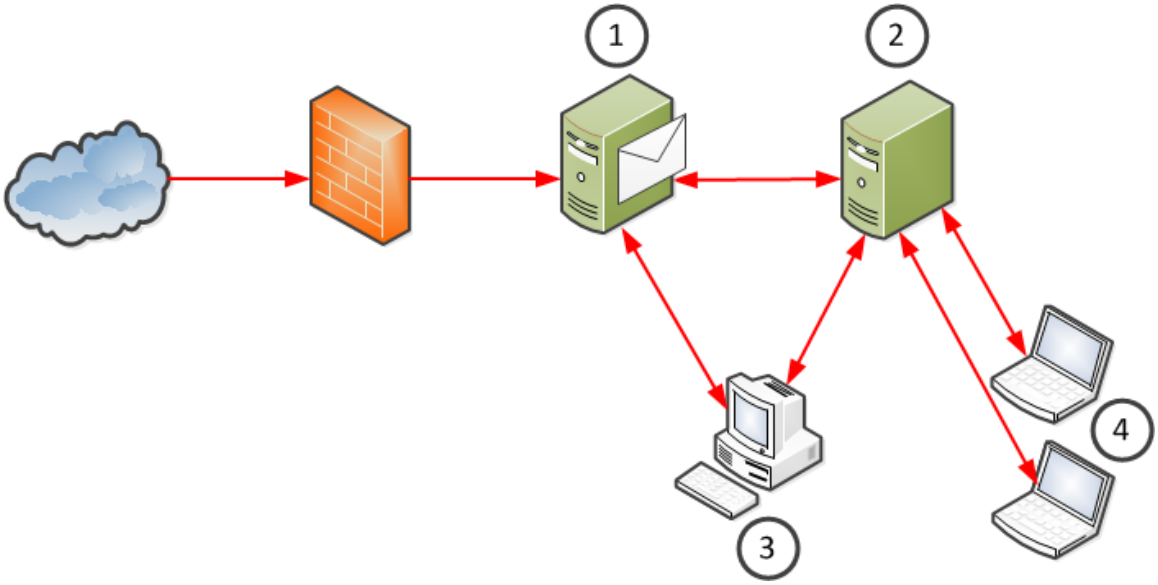


Abbildung 2-1 Workflow für MQM und unterstützte Produkte

Element	Beschreibung
1	Unterstütztes McAfee-Produkt
2	MQM-Server
3	E-Mail-Server
4	Administrator
5	Benutzer

Hochverfügbarkeit

Sie können MQM in einer Cluster-Umgebung mit zwei Knoten installieren, um die durchgehende Verfügbarkeit von MQM sicherzustellen.

MQM verwendet die Microsoft-Clusterdienste. Die von den Knoten gemeinsam verwendeten Konfigurationsdaten befinden sich auf dem Quorum-Laufwerk. Als Administrator erhalten Sie E-Mail-Benachrichtigungen, wenn ein Failover-Vorgang durchgeführt wird.

In einer Aktiv/Passiv-Konfiguration müssen Sie auf beiden Knoten den vollständigen Installationsvorgang durchführen.

Siehe auch

Konfigurieren eines Clusters unter Windows 2003 Server auf Seite 21
Konfigurieren eines Clusters unter Windows 2008 oder 2008 R2 Server auf Seite 22

Richtlinienverwaltung

McAfee ePO bietet eine skalierbare Plattform zur zentralen Verwaltung und Erzwingung von Richtlinien für Ihre McAfee-Sicherheitsprodukte und die Systeme, in denen sie sich befinden.

Die Software bietet außerdem umfassende Funktionen zur zentralisierten Berichterstellung und Produktbereitstellung.

Das vorliegende Handbuch enthält keine ausführlichen Informationen zum Installieren oder Verwenden der Software McAfee ePO. Informationen hierzu finden Sie im *McAfee ePolicy Orchestrator-Installationshandbuch* und im *McAfee ePolicy Orchestrator-Produkthandbuch*.

Siehe auch

Installieren von MQM auf dem McAfee ePO-Server auf Seite 26
Festlegen von Richtlinien in ePolicy Orchestrator auf Seite 31
Senden eines Aufrufs zur Agentenreaktivierung zum Abrufen neuer Eigenschaften bzw. Richtlinien auf Seite 33
Konfigurieren von Berichten auf Seite 33
Deinstallieren von McAfee Quarantine Manager mit ePolicy Orchestrator auf Seite 34

VMware-Unterstützung

Sie können MQM zur Verwendung in einer virtuellen Umgebung mit VMware 5.0 oder VMware 5.1 konfigurieren.

Die Abbildung zeigt ein Szenario für die Kommunikation zwischen einem unterstützten McAfee-Produkt und MQM in einer virtuellen Umgebung.

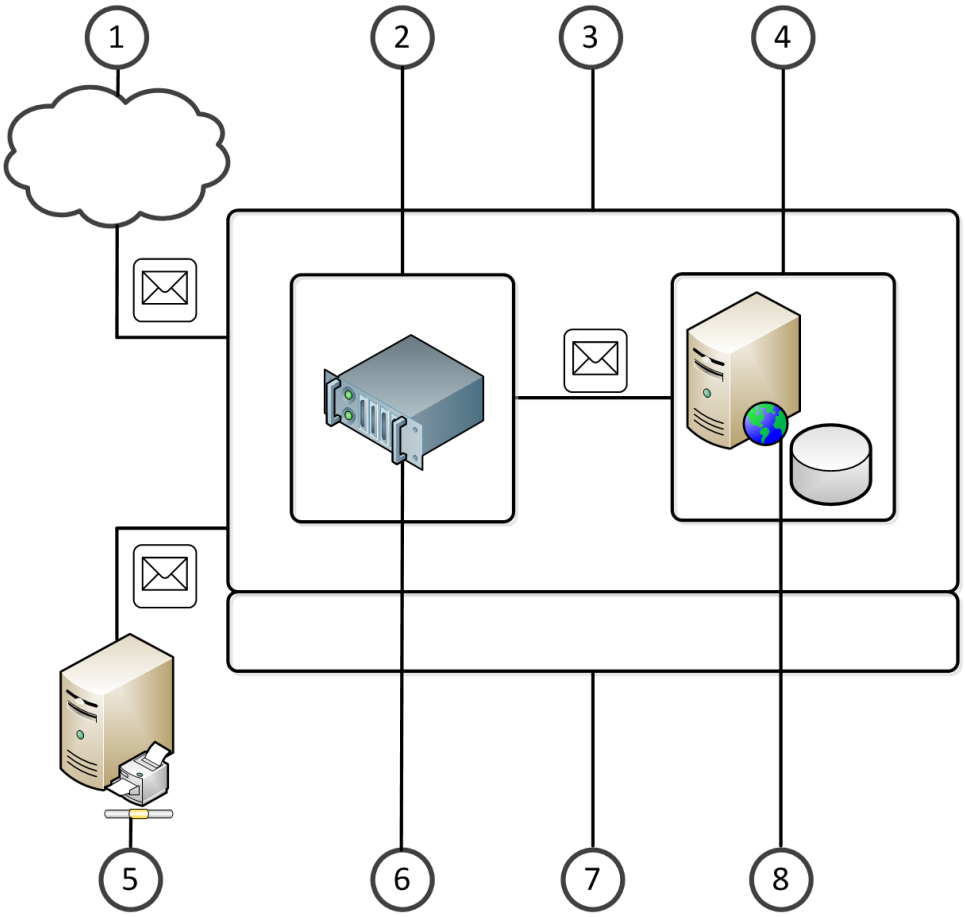


Abbildung 2-2 Szenario – Virtuelle Umgebung

Element	Beschreibung
1	Internet
2	Virtuelle Maschine 1
3	Physischer Hardware Dell Power Edge 1850 Blade-Server
4	Virtuelle Maschine 2
5	E-Mail-Server
6	Unterstütztes McAfee-Produkt
7	VMware ESX Server
8	MQM

Installation

Nachdem Sie sich für eine Bereitstellungsmethode entschieden haben, können Sie die Software anhand der Informationen in den folgenden Kapiteln installieren.

Kapitel 3 *Installation*

Kapitel 4 *Integrieren von McAfee Quarantine Manager in ePolicy Orchestrator*

Kapitel 5 *Arbeitsschritte nach der Installation*

3 Installation

Bereiten Sie die Installationsumgebung vor, und installieren Sie McAfee Quarantine Manager und die zugehörigen Komponenten eigenständig oder in einer Cluster-Umgebung. Wenn Sie die Software aus dem System entfernen oder ein Upgrade auf die aktuelle Version durchführen müssen, finden Sie in diesem Kapitel ebenfalls entsprechende Informationen.

Inhalt

- *Voraussetzungen*
- *Übersicht über die Installationsschritte*
- *Vorbereiten der Installationsumgebung*
- *Installieren von McAfee Quarantine Manager*
- *Installieren von McAfee Quarantine Manager in einer Cluster-Umgebung*
- *Deinstallieren von McAfee Quarantine Manager und Komponenten*
- *Upgrade auf die aktuelle Version von MQM*

Voraussetzungen

Vor dem Installieren von MQM muss die Arbeitsumgebung ordnungsgemäß eingerichtet sein.

Wichtige Hinweise

- Installieren Sie McAfee Security for Microsoft Exchange und MQM nicht auf demselben Computer.
- Installieren Sie MQM und McAfee ePO nicht auf demselben Computer.
- McAfee empfiehlt, MySQL für MQM, Microsoft SQL Server 2008 bzw. Microsoft SQL Server 2012 auf einem Computer zu installieren, auf dem sich kein anderes Datenbankprodukt befindet.
- Überprüfen Sie, ob MQM über das Netzwerk mit den McAfee-Produkten kommunizieren kann, mit denen es zusammenarbeitet.

Voraussetzungen

Element	Unterstützte Versionen
Unterstützte Server-Betriebssysteme	• Windows Server 2008 R2 SP2 (64 Bit) • Windows Server 2012 R2 SP2 (64 Bit)
Unterstützte Datenbanken	• MySQL Server Version 5.1 (im Download-Paket verfügbar) • Microsoft SQL Server 2008 SP1 Standard/Enterprise (64 Bit) • Microsoft SQL Server 2012 und Microsoft SQL Server 2012 R2 Die Datenbank kann auf demselben oder auf einem anderen Computer als MQM installiert werden.

Element	Unterstützte Versionen
Erforderliche Windows-Komponenten	Internetinformationsdienste 6.0 (IIS) oder höher
Arbeitsspeicher	2 GB RAM (Minimum)
Speicherplatz	160 GB mit NTFS-Dateisystem
Unterstützte Browser	• Microsoft Internet Explorer 7.0 oder höher • Mozilla Firefox 3.0 oder höher
Netzwerkanforderungen	Ethernet-Karte mit 100/1000 Mbit/s
Unterstützte McAfee-Produkte	• McAfee Email Gateway • McAfee Security for Microsoft Exchange • McAfee Security for Lotus Domino (Windows und Linux)
Unterstützte Upgrades	MQM 7.0.1
Unterstützte Verzeichnisdienste	• Microsoft Active Directory • IBM Domino Directory • Novell eDirectory • Open LDAP • Sun Java System Directory Server
Unterstützte Messaging-Server	• Novell GroupWise Mail Server • Sun Java System Messaging Server • Microsoft Exchange Server
Unterstützte E-Mail-Client-Software	• Microsoft Outlook 2007 oder Microsoft Outlook 2010 und Microsoft Outlook Express • IBM Lotus Notes 7.0 • Novell Groupwise-Mail-Client • Sun Java Convergence-Mail-Client
Prozessor	Zwei virtuelle Prozessoren

Übersicht über die Installationsschritte

Zur Vorbereitung der Umgebung, Installation der Software und Einrichtung der Datenbank müssen Sie die hier beschriebenen Installationsschritte durchführen.

1 Installieren und konfigurieren Sie die McAfee-Produkte, deren isolierte E-Mails von McAfee Quarantine Manager verwaltet werden sollen.

Mit McAfee Quarantine Manager können Sie die von McAfee Security for Microsoft Exchange und McAfee Email Gateway isolierten E-Mails verwalten. Informationen zur Installation und Konfiguration finden Sie in der jeweiligen Produktdokumentation.

2 Vergewissern Sie sich, dass Ihr System die Anforderungen erfüllt.

3 Installieren und konfigurieren Sie eine Datenbank für McAfee Quarantine Manager.

4 Installieren Sie den McAfee Quarantine Manager-Server.

5 (Optional) Installieren Sie die McAfee Quarantine Manager-Erweiterungen, wenn Sie das Paket in McAfee ePolicy Orchestrator integrieren möchten.

6 Testen Sie Ihre Installation.

Siehe auch

Installieren von MySQL for McAfee Quarantine Manager auf Seite 19
Installieren von McAfee Quarantine Manager auf Seite 21
Hinzufügen oder Importieren von Domänen zu McAfee Quarantine Manager auf Seite 47
Verwalten der Server-Konfigurationen auf Seite 79
Verwalten von Benutzerkonten auf Seite 4
Verwalten von Tasks auf Seite 4
Verwaltung von Blacklists und Whitelists auf Seite 5
Konfigurieren der Datenbank auf Seite 37
Zuweisen von Domänen zu Domänenadministratoren auf Seite 49
Testen von verbundenen McAfee-Produkten auf Seite 95
Ändern von Domänenkonfigurationen auf Seite 49

Vorbereiten der Installationsumgebung

Richten Sie eine geeignete Datenbankumgebung für die Installation von McAfee Quarantine Manager ein.

Konfigurieren der Microsoft SQL Server-Datenbank

Sie können die Einstellungen für die vorhandene Microsoft SQL Server-Datenbank für McAfee Quarantine Manager konfigurieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Aktivieren Sie die Authentifizierung im **gemischten Modus** auf dem SQL-Server.

2 Erstellen Sie einen Datenbankbenutzer mit der **Server-Rolle** `sysadmin`.

3 Erstellen Sie eine leere Datenbank, die mit McAfee Quarantine Manager verwendet werden muss, und weisen Sie den erstellten Benutzer als Besitzer dieser Datenbank zu.

4 Installieren Sie Microsoft SQL Server Native Client auf dem McAfee Quarantine Manager-Server.

Installieren von MySQL for McAfee Quarantine Manager

Die MySQL-Datenbank und McAfee Quarantine Manager können auf zwei verschiedenen Servern oder auf dem gleichen Server installiert werden.

Die unterstützten MySQL-Datenbanken sind MySQL for McAfee Quarantine Manager (im Paket enthalten), MySQL 5.1 for Windows und MySQL 5.1 for Linux.

McAfee empfiehlt, die Software MySQL for McAfee Quarantine Manager auf einem Computer zu installieren, auf dem kein anderer Datenbank-Server installiert ist.

Vorgehensweise

1 Extrahieren Sie die ZIP-Datei aus dem Verzeichnis **MySQL for McAfee Quarantine Manager** in ein temporäres Verzeichnis, und doppelklicken Sie auf **SETUP.EXE**.

2 Klicken Sie auf **Weiter**, und befolgen Sie die auf dem Bildschirm angezeigten Anweisungen.

3 Legen Sie im Dialogfeld **Datenbankservereinstellungen** die folgenden Konfigurationseinstellungen für **MySQL for McAfee Quarantine Manager** fest:

- **Benutzername**: Der Standard-Benutzername ist `root`.
- **Kennwort**: Das Standard-Kennwort ist `root`.
- **Datenbankname**: Der Standard-Datenbankname ist `mqm`.
- **Port-Nummer**: Die Standard-Port-Nummer ist `3306`.
- McAfee Quarantine Manager-Super-Administrator **Benutzername** und **Kennwort**: Der Standard-Benutzername lautet `super@mqm.com`, und das Standard-Kennwort ist `super123`.

4 Klicken Sie im Dialogfeld **Bereit zur Installation** auf **Weiter**.

5 Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Konfigurieren von MySQL 5.1 für Linux oder Microsoft Windows

Konfigurieren Sie die Parameter für die vorhandene MySQL 5.1-Datenbank für McAfee Quarantine Manager.

Fügen Sie in der Datei „MY.CNF"/„MY.INI" die folgenden Parameter hinzu:

Parameter	Wert
default_storage_engine	InnoDB
lower_case_table_names	1
max_allowed_packet	Mindestens 150 M (wobei M für MB steht)
max_connections	Mindestens 100
innodb_file_per_table	1

Folgende Parameter-Einstellungen werden empfohlen.

Parameter	Wert
max_allowed_packet	Mindestens 1024 M (wobei M für MB steht)
max_connections	500
innodb_flush_log_at_trx_commit	0
innodb_support_xa	0
innodb_locks_unsafe_for_binlog	1
innodb_doublewrite	0

- Keiner der Parameter für „innodb_*" darf auskommentiert sein.
- Eine externe MySQL-Datenbank unter Linux oder Microsoft Windows wird nur mit dem InnoDB-Modul unterstützt.

Installieren von McAfee Quarantine Manager

Führen Sie die Schritte zur Ersteinrichtung von McAfee Quarantine Manager durch, und legen Sie die Port-Nummer fest, unter der die McAfee Quarantine Manager-Website durch die Internetinformationsdienste gehostet wird.

> **Bevor Sie beginnen**
>
> Vergewissern Sie sich, dass Microsoft SQL Server Native Client auf dem McAfee Quarantine Manager-Server installiert ist, falls Sie die auf einem anderen Computer installierte Anwendung Microsoft SQL Server 2005/2008 verwenden möchten.

Vorgehensweise

1. Extrahieren Sie aus dem Verzeichnis McAfee Quarantine Manager die ZIP-Datei McAfee Quarantine Manager in ein temporäres Verzeichnis, und doppelklicken Sie auf **SETUP.EXE**.
2. Befolgen Sie nun die auf dem Bildschirm angezeigten Anweisungen zum Installieren der Software.
3. Geben Sie die Port-Nummer an, unter der die McAfee Quarantine Manager-Website durch die Internetinformationsdienste gehostet wird. Der Standardwert beträgt `80`.
4. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
5. Klicken Sie auf **Ja**, um den Computer neu zu starten.

Installieren von McAfee Quarantine Manager in einer Cluster-Umgebung

Sie können McAfee Quarantine Manager in einer Cluster-Umgebung mit zwei Knoten installieren, um die durchgehende Verfügbarkeit von McAfee Quarantine Manager sicherzustellen.

Konfigurieren eines Clusters unter Windows 2003 Server

Sie können mit McAfee Quarantine Manager eine Cluster-Umgebung auf Computern unter Windows 2003 Server einrichten.

Vorgehensweise

1. Öffnen Sie die Microsoft Cluster-Administrator-Konsole.
2. Wählen Sie **Clustergruppe** | **Neu** | **Ressource** aus.
3. Geben Sie die folgenden Informationen an:
   - **Name**: Geben Sie einen geeigneten Namen für den Cluster-Dienst an.
   - **Beschreibung**: Geben Sie eine Beschreibung für den Cluster-Dienst an.
   - **Ressourcentyp**: Wählen Sie **McAfee MQM Cluster Framework** aus.
   - **Gruppe**: Wählen Sie die entsprechende Gruppe aus.

4 Wählen Sie **Mögliche Besitzer** aus.

Der mögliche Besitzer ist der Cluster-Knoten, auf dem die Ressourcen online geschaltet werden können. Fügen Sie beide Knoten als **Mögliche Besitzer** hinzu.

5 Fügen Sie unter **Abhängigkeiten** das Quorum-Laufwerk zur Angabe der Ressourcenabhängigkeit hinzu.

Vergewissern Sie sich, dass der Ressourcentyp für die Gruppe als „Physischer Datenträger" vorhanden ist. Der Ressourcentyp wird vom McAfee Quarantine Manager Cluster Framework-Dienst zum Speichern der gemeinsam genutzten Daten verwendet.

Konfigurieren eines Clusters unter Windows 2008 oder 2008 R2 Server

Sie können mit McAfee Quarantine Manager eine Cluster-Umgebung auf Computern unter Windows 2008 oder 2008 R2 Server einrichten.

Vorgehensweise

1 Öffnen Sie die Failovercluster-Manager-Konsole, und wählen Sie **Dienste und Anwendungen** | **Dienst oder Anwendung konfigurieren** aus.

2 Klicken Sie unter **Dienst oder Anwendung auswählen** die Option **Anderer Server** aus.

3 Geben Sie im Dialogfeld **Clientzugriffspunkt** den Namen und die IP-Adresse für den Zugriff auf die MQM-Ressourcen an.

4 Wählen Sie den Speicher aus, der vom MQM-Dienst zum Speichern der gemeinsam genutzten Daten verwendet wird.

5 Wählen Sie als **Ressourcentyp** das **McAfee MQM Cluster Framework** aus.

6 Wählen Sie den neu konfigurierten Dienst aus, und wählen Sie die Eigenschaften für das **Neue McAfee MQM Cluster Framework** aus.

7 Klicken Sie auf die Registerkarte **Eigenschaften**.

8 Geben Sie für das **freigegebene Datenlaufwerk** den **Laufwerkspfad** zum Speichern der von MQM freigegebenen Daten an.

9 Übernehmen Sie die Konfiguration, wählen Sie den neu konfigurierten Dienst aus, und klicken Sie dann auf **Diesen Dienst oder diese Anwendung online schalten**.

10 Wählen Sie **Failovercluster-Manager** | **Dienste und Anwendungen** | **<MQM-Ressource>** aus, und doppelklicken Sie dann auf **Neues McAfee MQM Cluster Framework**.

11 Aktivieren Sie **Ein erfolgloser Neustart wirkt sich negativ auf alle Ressourcen im Dienst oder in der Anwendung aus**.

12 Geben Sie auf der Registerkarte **Richtlinie** unter **MQM-Ressource** einen Wert für **Maximale Anzahl von Neustarts im angegebenen Zeitraum** an.

13 Vergewissern Sie sich, dass die Abhängigkeiten hinzugefügt wurden, sodass das Festplattenlaufwerk aktiv wird, bevor die <*MQM-Ressource*> online geschaltet wird.

Deinstallieren von McAfee Quarantine Manager und Komponenten

Zum Entfernen der McAfee Quarantine Manager-Software von Ihrem Computer müssen Sie die McAfee Quarantine Manager-Software und die MySQL-Software entfernen.

Aufgaben

- *Deinstallieren der McAfee Quarantine Manager-Software* auf Seite 23
  Sie können die McAfee Quarantine Manager-Software von dem Server, auf dem sie installiert ist, entfernen.
- *Deinstallieren von MySQL for McAfee Quarantine Manager* auf Seite 23
  Sie können das Dienstprogramm MySQL for McAfee Quarantine Manager von dem Computer, auf dem es installiert ist, entfernen.

Deinstallieren der McAfee Quarantine Manager-Software

Sie können die McAfee Quarantine Manager-Software von dem Server, auf dem sie installiert ist, entfernen.

Vorgehensweise

1 Klicken Sie auf **Start** | **Einstellungen** | **Systemsteuerung** | **Programme hinzufügen oder entfernen** (Systemlisten | SSO-Katalog).

2 Wählen Sie **McAfee Quarantine Manager** aus, und klicken Sie dann auf **Entfernen**.

3 (Optional) Wählen Sie **MQM-Daten ebenfalls entfernen** aus, wenn die zum Speichern isolierter Objekte erstellte Datenbank ebenfalls entfernt werden soll.

Bei Auswahl dieser Option wird die McAfee Quarantine Manager-Datenbank unwiderruflich gelöscht.

Deinstallieren von MySQL for McAfee Quarantine Manager

Sie können das Dienstprogramm MySQL for McAfee Quarantine Manager von dem Computer, auf dem es installiert ist, entfernen.

Vorgehensweise

1 Klicken Sie auf **Start** | **Einstellungen** | **Systemsteuerung** | **Programme hinzufügen oder entfernen** für diese Domäne konfiguriert wurde.

2 Wählen Sie **MySQL for McAfee Quarantine Manager** aus, und klicken Sie dann auf **Entfernen**.

Upgrade auf die aktuelle Version von MQM

Sie sollten für ältere Versionen der MQM-Software ein Upgrade auf die aktuelle Version durchführen.

Sie können ein Upgrade von McAfee Quarantine Manager 7.0.1 auf McAfee Quarantine Manager 7.1.0 durchführen.

Vorgehensweise

1 Sichern Sie zunächst die vorhandene Datenbank.

Starten Sie nach der Durchführung der Datenbanksicherung den McAfee Quarantine Manager-Dienst.

2 Installieren Sie die Komponente MySQL for McAfee Quarantine Manager.

Wenn Sie eine Microsoft SQL-Datenbank verwenden, können Sie diesen Schritt überspringen.

3 Installieren Sie die aktuelle Version von McAfee Quarantine Manager.

4 Löschen Sie anschließend die Browser-Cookies und die temporären Internet-Dateien, damit die Benutzeroberfläche ordnungsgemäß dargestellt werden kann, und starten Sie den Browser dann neu.

5 Konfigurieren und testen Sie nun die Datenbank.

Wenn Sie versuchen, sich während der Datenbankmigration bei MQM anzumelden, wird die folgende Meldung angezeigt:
Zurzeit wird eine Datenbankmigration durchgeführt. Bitte versuchen Sie es nach einiger Zeit erneut.
Migrationsstatus: <Y> von <X> Tabellen abgeschlossen.

6 Nachdem die Datenmigration abgeschlossen und die Datenbank ordnungsgemäß konfiguriert wurde, können Sie sich bei MQM anmelden.

McAfee empfiehlt im Anschluss an die Datenmigration einen Neustart der MQM-Dienste, damit die Benutzeroberfläche ordnungsgemäß dargestellt wird.

7 Testen Sie nun die Installation.

Siehe auch

Sichern der Datenbank auf Seite 86
Installieren von MySQL for McAfee Quarantine Manager auf Seite 19
Installieren von McAfee Quarantine Manager auf Seite 21
Konfigurieren der Datenbank auf Seite 37
Testen der Installation auf Seite 38

4 Integrieren von McAfee Quarantine Manager in ePolicy Orchestrator

ePolicy Orchestrator bietet eine skalierbare Plattform zur zentralen Verwaltung und Erzwingung von Richtlinien für Ihre McAfee-Sicherheitsprodukte und die Systeme, in denen sie sich befinden. Die Software bietet außerdem umfassende Funktionen zur zentralisierten Berichterstellung und Produktbereitstellung.

McAfee empfiehlt, dass Sie sich mit der Software ePolicy Orchestrator vertraut machen, ehe Sie den Integrationsvorgang beginnen.

Das vorliegende Handbuch enthält keine ausführlichen Informationen zum Installieren oder Verwenden der Software ePolicy Orchestrator. Informationen hierzu finden Sie im *ePolicy Orchestrator-Produkthandbuch* und im *ePolicy Orchestrator-Installationshandbuch*.

Inhalt

- *Vorbereitungsschritte für die Integration*
- *Bereitstellen des McAfee Quarantine Manager-Pakets und der Erweiterungen*
- *Festlegen von Richtlinien in ePolicy Orchestrator*
- *Senden eines Aufrufs zur Agentenreaktivierung zum Abrufen neuer Eigenschaften bzw. Richtlinien*
- *Konfigurieren von Berichten*
- *Deinstallieren von McAfee Quarantine Manager mit ePolicy Orchestrator*

Vorbereitungsschritte für die Integration

Vor dem Integrieren von McAfee Quarantine Manager und McAfee ePO müssen Sie alle ggf. vorhandenen älteren Versionen des McAfee Quarantine Manager-Pakets und der zugehörigen Erweiterungen entfernen.

Pakete und Erweiterungen	Schritte
• **McAfee Quarantine Manager-Paket** • **MySQL for McAfee Quarantine Manager-Paket**	So entfernen Sie die Software-Pakete: 1 Klicken Sie auf **Menü** | **Software** | **Master-Repository**. 2 Wählen Sie das jeweilige Paket aus, und klicken Sie auf **Löschen**.
• **McAfee Quarantine Manager-Richtlinienerweiterung** • **McAfee Quarantine Manager-Berichtserweiterung**	So entfernen Sie die Produkterweiterungen: 1 Klicken Sie auf **Menü** | **Software** | **Erweiterungen**. 2 Wählen Sie die jeweilige Erweiterung aus, und klicken Sie auf **Entfernen**.

Bereitstellen des McAfee Quarantine Manager-Pakets und der Erweiterungen

Nach dem Bereitstellen der McAfee Quarantine Manager-Pakete und der zugehörigen Erweiterungen auf Client-Computern können Sie diese mithilfe von McAfee ePO verwalten.

Installieren von MQM auf dem McAfee ePO-Server

Extrahieren Sie das MQM-Paket auf dem McAfee ePO-Server.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Erstellen Sie ein temporäres Verzeichnis auf der lokalen Festplatte.
3. Extrahieren Sie das MQM-Paket in ein temporäres Verzeichnis. Dort sind nun folgende Ordner vorhanden:
   - **McAfee Quarantine Manager**
   - **MySQL for McAfee Quarantine Manager**
   - **ePO**

   Installieren Sie mithilfe der im **ePO**-Ordner enthaltenen Richtlinien-, Berichts- und Hilfe-ZIP-Dateien die McAfee ePO-Erweiterungen.

Bereitstellen von McAfee Agent auf Client-Computern

McAfee Agent ist die verteilte Komponente von McAfee ePO, die auf jedem System im Netzwerk installiert werden muss, das Sie verwalten möchten.

Bevor Sie beginnen

McAfee Agent empfiehlt, vor dem Bereitstellen von McAfee die Kommunikation zwischen dem Server und den Systemen sowie den Zugriff auf das standardmäßige Administrator-Freigabeverzeichnis zu überprüfen. Außerdem müssen Sie möglicherweise Firewall-Ausnahmen erstellen.

Der Agent erfasst Daten und sendet sie an den McAfee ePO-Server. Außerdem installiert und aktualisiert er die Produkte auf den Endgeräten und wendet Ihre Richtlinien für Endgeräte an. McAfee ePO verwaltet nur Systeme, auf denen McAfee Agent installiert ist.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** und dann in der Menüleiste auf **Systeme**.
3. Markieren Sie eine Gruppe. Wenn diese Gruppe keine Systeme, aber Untergruppen mit Systemen enthält, klicken Sie auf die Dropdown-Liste **Filter**, und wählen Sie **Diese Gruppe und alle Untergruppen** aus.

4 Wählen Sie mindestens ein System in der Liste aus, und klicken Sie dann auf **Aktionen** | **Agent** | **Agenten ausbringen** (Systemlisten | SSO-Katalog).

5 Geben Sie Anmeldeinformationen für eine Rolle ein, die über Rechte zum Installieren von Software auf Client-Systemen verfügt (z. B. ein Domänenadministrator), und klicken Sie dann auf **OK**.

Es dauert einige Minuten, bis McAfee Agent installiert ist und die Installationspakete für die Endgerätprodukte von den Client-Systemen abgerufen und ausgeführt wurden. Bei der Erstinstallation legt der Agent einen zufälligen Zeitraum von maximal zehn Minuten fest, innerhalb dessen eine Verbindung mit dem McAfee ePO-Server hergestellt werden muss, damit Richtlinien und Tasks abgerufen werden können.

McAfee Agent kann jedoch auch auf verschiedene andere Arten bereitgestellt werden. Weitere Informationen hierzu finden Sie im *Produkthandbuch von ePolicy Orchestrator* bzw. in der Online-Hilfe.

Einchecken des McAfee Quarantine Manager-Pakets

Checken Sie das McAfee Quarantine Manager-Paket in das McAfee ePolicy Orchestrator-Master-Repository ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

2 Klicken Sie auf **Menü** | **Software** | **Master-Repository** | **Aktionen** | **Paket einchecken** (Systemlisten | SSO-Katalog).

Daraufhin öffnet sich die Seite **Paket**.

3 Wählen Sie als **Pakettyp** den Eintrag **Produkt oder Aktualisierung (.ZIP)** aus, und navigieren Sie zu der im Ordner McAfee Quarantine Manager gespeicherten Datei MQM710Server.zip.

4 Klicken Sie auf **Weiter**.

Nun öffnet sich die Seite **Paketoptionen**, auf der Informationen zum Paket angezeigt werden.

5 Wählen Sie einen Zweig aus.

6 Wählen Sie unter **Optionen** die gewünschten Optionen aus, und klicken Sie dann auf **Speichern**.

Einchecken des Pakets „MySQL for McAfee Quarantine Manager"

Checken Sie das Paket „MySQL for McAfee Quarantine Manager" in das ePolicy Orchestrator-Master-Repository ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

2 Klicken Sie auf **Menü** | **Software** | **Master-Repository** | **Aktionen** | **Paket einchecken** (Systemlisten | SSO-Katalog).

Daraufhin öffnet sich die Seite **Paket**.

3 Wählen Sie als **Pakettyp** den Eintrag **Produkt oder Aktualisierung (.ZIP)** aus, und navigieren Sie zu der im Ordner **MySQL for McAfee Quarantine Manager** gespeicherten Datei MQM710MySQL.zip.

4 Klicken Sie auf **Weiter**.

Nun öffnet sich die Seite **Paketoptionen**, auf der Informationen zum Paket angezeigt werden.

5 Wählen Sie einen Zweig aus.

6 Wählen Sie unter **Optionen** die gewünschten Optionen aus, und klicken Sie dann auf **Speichern**.

Bereitstellen der Komponente MySQL for McAfee Quarantine Manager

Fügen Sie die Komponente MySQL for McAfee Quarantine Manager zu Client-Computern hinzu, die durch McAfee ePO verwaltet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

2 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** (Systemlisten | SSO-Katalog).

3 Wählen Sie einen Knoten aus, und klicken Sie auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern** für diese Domäne konfiguriert wurde.

4 Erstellen Sie einen Task.

   a Klicken Sie auf **Neuer Task**.

   b Geben Sie auf der Seite **Generator für Client-Tasks** den Namen des Tasks und ggf. Anmerkungen dazu ein.

   c Wählen Sie in der Dropdown-Liste **Typ** den Eintrag **Produktbereitstellung** aus.

   d Klicken Sie auf **Weiter**.

5 Wählen Sie unter **Konfiguration** die **Zielplattformen** aus.

6 Wählen Sie unter **Produkte und Komponenten** im Dropdown-Menü die Komponente **MySQL for McAfee Quarantine Manager 7.1.x.x** aus, und wählen Sie dann **Installieren** als **Aktion** aus.

Sie können auch Befehlszeilenargumente zur Installation von MySQL for McAfee Quarantine Manager mit benutzerdefinierten Werten angeben. Bei Angabe mehrerer Parameter müssen Sie diese durch Leerzeichen trennen.

Beispiel: `INSTALLDIR="C:\MySQL" SUPERID="superduper@mqm.com" SUPERIDPWD="superduper123"`

Parameter	Beispiel	Beschreibung
INSTALLDIR	INSTALLDIR="C:\MySQL"	MySQL wird im angegebenen Ordner installiert.
MYSQLUSER	MYSQLUSER="root123"	Hiermit wird der Benutzernamen für MySQL festgelegt.
MYSQLPASSWORD	MYSQLPASSWORD="root123"	Hiermit wird das Kennwort für MySQL festgelegt.
MYSQLDBNAME	MYSQLDBNAME="mymqm"	Hiermit wird der Name der MySQL-Datenbank festgelegt.
MYSQLPORT	MYSQLPORT=3361	Hiermit wird die Port-Nummer für MySQL festgelegt.
SUPERID	SUPERID="superduper@mqm.com"	Hiermit wird die E-Mail-Adresse des Super-Administrators festgelegt.
SUPERIDPWD	SUPERIDPWD="superduper123"	Hiermit wird das Kennwort des Super-Administrators festgelegt.

7 Aktivieren bzw. deaktivieren Sie unter **Optionen** das Kontrollkästchen **Bei jeder Richtlinienerzwingung ausführen (nur Windows)**.

8 Klicken Sie auf **Weiter**, und planen Sie den Task nach Bedarf.

9 Klicken Sie auf **Weiter**, um eine Zusammenfassung des Tasks anzuzeigen.

10 Klicken Sie auf **Speichern**, und senden Sie einen Aufruf zur Agentenreaktivierung.

Bereitstellen von MQM auf Client-Computern

Sie können eine Standardinstallation unter Verwendung der MQM-Standardeinstellungen auf den Client-Computern durchführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

2 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** (Systemlisten | SSO-Katalog).

3 Wählen Sie einen Knoten aus, und klicken Sie dann auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern** (Systemlisten | SSO-Katalog).

4 Erstellen Sie einen Task.

a Klicken Sie auf **Neuer Task**.

b Geben Sie auf der Seite **Generator für Client-Tasks** den Namen des Tasks und ggf. Anmerkungen dazu ein.

c Wählen Sie in der Dropdown-Liste **Typ** den Eintrag **Produktbereitstellung** aus.

d Klicken Sie auf **Weiter**.

5 Wählen Sie unter **Konfiguration** die **Zielplattformen** aus.

6 Wählen Sie unter **Auszubringende Produkte** in der Dropdown-Liste **McAfee Quarantine Manager 7.1.x.x** und dann **Installieren** als **Aktion** aus.

Sie können auch Befehlszeilenargumente für eine benutzerdefinierte Installation von McAfee Quarantine Manager auf dem Client-Computer angeben, wenn Sie andere als die Standardwerte verwenden möchten. Bei Angabe mehrerer Parameter müssen Sie diese durch Leerzeichen trennen.

Beispiel: `INSTALLDIR="C:\MQM" REBOOTREQUIRED=1`

Tabelle 4-1 Befehlszeilenargumente für das Installationsprogramm

Parameter	Beispiel	Beschreibung
INSTALLDIR	`INSTALLDIR="C:\MQM"`	Hiermit wird McAfee Quarantine Manager im angegebenen Ordner installiert.
REBOOTREQUIRED	`REBOOTREQUIRED=1`	Der Client-Computer wird nach der Installation neu gestartet.

7 Aktivieren bzw. deaktivieren Sie unter **Optionen** das Kontrollkästchen **Bei jeder Richtlinienerzwingung ausführen (nur Windows)**.

8 Klicken Sie auf **Weiter**, und planen Sie den Task nach Bedarf.

9 Klicken Sie auf **Weiter**, um eine Zusammenfassung des Tasks anzuzeigen.

10 Klicken Sie auf **Speichern**, und senden Sie einen Aufruf zur Agentenreaktivierung.

Installieren der McAfee Quarantine Manager-Richtlinienerweiterung

Installieren Sie die McAfee Quarantine Manager-Richtlinienerweiterung, um die MQM-Clients per Remote-Zugriff verwalten zu können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

2 Klicken Sie auf **Menü** | **Software** | **Erweiterungen** | **Erweiterung installieren** (Systemlisten | SSO-Katalog).

Daraufhin öffnet sich das Dialogfeld **Erweiterung installieren**.

3 Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei MQM710POLICIES.zip aus, und klicken Sie dann auf **OK**.

Wenn Sie mehrere MQM-Server mit McAfee ePO verwalten, empfiehlt McAfee, jedem Server eine eigene Richtlinie für die Datenbankkonfiguration zuzuweisen. So vermeiden Sie Konflikte zwischen den Servern, wenn diese versuchen, auf dieselbe Datenbank zuzugreifen.

Installieren der McAfee Quarantine Manager-Berichtserweiterung

Installieren Sie die MQM-Berichtserweiterung auf dem McAfee ePO-Server, um Abfragen auf den MQM-Clients durchführen zu können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Software** | **Erweiterungen** | **Erweiterung installieren** für diese Domäne konfiguriert wurde.

   Daraufhin öffnet sich das Dialogfeld **Erweiterung installieren**.
3. Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei MQM710REPORTS.zip aus, und klicken Sie dann auf **OK**.

Installieren der MQM-Hilfeerweiterung

Installieren Sie die MQM-Hilfeerweiterung auf dem McAfee ePO-Server, um das McAfee ePO-Hilfesystem um das *McAfee Quarantine Manager-Produkthandbuch* und das Online-Hilfesystem zu ergänzen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Software** | **Erweiterungen** | **Erweiterung installieren** für diese Domäne konfiguriert wurde.

   Daraufhin öffnet sich das Dialogfeld **Erweiterung installieren**.
3. Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei HELP_MQM_710.zip aus, und klicken Sie dann auf **OK**.

Festlegen von Richtlinien in ePolicy Orchestrator

Über die ePolicy Orchestrator-Konsole können Sie Richtlinien für Gruppen von Computern bzw. für einen einzelnen Computer erzwingen.
Diese Richtlinien setzen die Konfigurationen einzelner Computer außer Kraft. Informationen zu Richtlinien und deren Erzwingung finden Sie im Produkthandbuch zu *McAfee ePolicy Orchestrator* .

Wählen Sie vor der Konfiguration von Richtlinien die Gruppe von Computern aus, für die Sie McAfee Quarantine Manager-Richtlinien ändern möchten. Sie können die Richtlinien für McAfee Quarantine Manager über die Seiten und Registerkarten im Detailbereich der ePolicy Orchestrator-Konsole ändern. Diese Seiten ähneln den Seiten, die Sie über die Benutzeroberfläche für Administratoren von McAfee Quarantine Manager aufrufen können.

Nachdem Sie die entsprechenden Richtlinien geändert und die Änderungen für den entsprechenden Computer bzw. die Gruppe von Computern gespeichert haben, können Sie die neuen Einstellungen über McAfee Agent bereitstellen.

Aufgaben

- *Erstellen und Bearbeiten von Richtlinien* auf Seite 32
  Sie können Richtlinien erstellen, bearbeiten und löschen sowie einer bestimmten Gruppe in der **Systemstruktur** zuweisen.
- *Erzwingen von Richtlinien* auf Seite 32
  Sie können eine Richtlinie für mehrere verwaltete Systeme innerhalb einer Gruppe erzwingen.

Erstellen und Bearbeiten von Richtlinien

Sie können Richtlinien erstellen, bearbeiten und löschen sowie einer bestimmten Gruppe in der **Systemstruktur** zuweisen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** (Systemlisten | SSO-Katalog).

   Daraufhin öffnet sich die Seite **Systemstruktur**.
3. Klicken Sie auf **Zugewiesene Richtlinien**.
4. Wählen Sie als **Produkt** den Eintrag **McAfee Quarantine Manager 7.1** aus.

   Im unteren Fensterbereich wird nun eine Liste der von MQM verwalteten Richtlinien angezeigt.
5. Navigieren Sie zur gewünschten Richtlinie, und klicken Sie dann neben der Richtlinie auf **Zuweisung bearbeiten**. Daraufhin öffnet sich die Seite mit der Richtlinienzuweisung für die ausgewählte Gruppe.
6. Klicken Sie nach Bedarf auf **Richtlinie bearbeiten** oder auf **Neue Richtlinie**.

   Wenn Sie auf **Neue Richtlinie** klicken, öffnet sich das Dialogfeld **Neue Richtlinie erstellen**. Wählen Sie in der Dropdown-Liste **Richtlinie auf Grundlage dieser vorhandenen Richtlinie erstellen** die gewünschte Richtlinie aus, geben Sie einen Namen ein, und klicken Sie dann auf **OK**. Daraufhin öffnet sich der Assistent zum Erstellen neuer Richtlinien.
7. Bearbeiten Sie die Richtlinieneinstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Erzwingen von Richtlinien

Sie können eine Richtlinie für mehrere verwaltete Systeme innerhalb einer Gruppe erzwingen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Wählen Sie **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die gewünschte Gruppe bzw. die gewünschten Systeme aus.
3. Klicken Sie auf **Zugewiesene Richtlinien**, und wählen Sie anschließend im Dropdown-Menü **Produkt** den Eintrag **McAfee Quarantine Manager 7.1** aus.
4. Wählen Sie die gewünschte **Kategorie** aus, und klicken Sie auf **Zuweisung bearbeiten**.
5. Wählen Sie im Dropdown-Menü **Zugewiesene Richtlinie** die gewünschte Richtlinie aus, und klicken Sie dann auf **Speichern**.
6. Wählen Sie die Systeme erneut aus.
7. Senden Sie einen Aufruf zur Agentenreaktivierung.

   Sie können erst MQM-Richtlinien erstellen und erzwingen sowie Berichte anzeigen, nachdem die MQM-Erweiterungsdateien hinzugefügt wurden.

Senden eines Aufrufs zur Agentenreaktivierung zum Abrufen neuer Eigenschaften bzw. Richtlinien

Zum Abrufen neuer Eigenschaften oder Richtlinien können Sie mit McAfee ePO einen Aufruf zur Agentenreaktivierung senden.

Alle Systeme im Netzwerk werden über die Registerkarte **Systeme** verwaltet. Die **Systemstruktur** enthält alle vom McAfee ePO-Server verwalteten Systeme. Sie bildet die grundlegende Verwaltungsoberfläche für die Richtlinien und Tasks der Systeme und kann zum Organisieren bzw. Sortieren der Systeme in logische Gruppen verwendet werden.

Eigene Organisation ist das Stammverzeichnis der **Systemstruktur**. Es enthält eine **Sammelgruppe**, in der die Systeme gespeichert werden, deren Standorte vom Server nicht ermittelt werden können. Abhängig von der Methode, mit der die Segmente (Systeme) in der **Systemstruktur** erstellt und verwaltet werden, werden die Systeme vom der Server anhand unterschiedlicher Merkmale in der **Systemstruktur** angeordnet.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** für diese Domäne konfiguriert wurde.
3. Wählen Sie in der **Systemstruktur** eine Gruppe aus.
4. Wählen Sie die Gruppe **Computername** aus.
5. Wählen Sie **Aktionen** | **Agent** | **Agenten reaktivieren** aus.
6. Wählen Sie auf der Seite **McAfee Agent reaktivieren** als Reaktivierungsaufruftyp **Agenten-Reaktivierung** aus, und legen Sie dann einen Zeitraum für den Zufallsgenerator (0–60 Minuten) fest. Innerhalb dieses Zeitraums reagieren die Systeme auf den Reaktivierungsaufruf.
7. Wenn die Agenten sämtliche Eigenschaften senden sollen und nicht nur diejenigen, die sich seit der letzten Agent-Server-Kommunikation geändert haben, aktivieren Sie die Option **Vollständige Produkteigenschaften abrufen**.
8. Klicken Sie auf **OK**.

Wenn Sie den Status des Aufrufs zur Agentenreaktivierung anzeigen möchten, wählen Sie **Menü** | **Automatisierung** | **Server-Task-Protokoll** aus.

Konfigurieren von Berichten

Ein Bericht ist eine vordefinierte Abfrage der McAfee ePO-Datenbank, bei der eine visuelle Darstellung der Daten ausgegeben wird.

McAfee ePO verfügt über eigene Abfrage- und Berichterstellungsfunktionen. McAfee bietet eine Reihe von Standardabfragen. Sie können auch neue Abfragen erstellen und alle Abfragen im Zusammenhang mit MQM bearbeiten sowie verwalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich beim McAfee ePO-Server als Administrator an.

> Sie können die mit McAfee ePO installierten vordefinierten Abfragen verwenden oder eigene Abfragen erstellen.

2 Wählen Sie den Abfrageergebnistyp aus.

   a Wählen Sie **Menü** | **Abfragen und Berichte** | **Aktionen** | **Neu** aus, oder wählen Sie eine vorhandene Abfrage in der Liste aus, und klicken Sie dann auf **Bearbeiten**.

   b Klicken Sie auf der Seite **Abfrage-Generator** in der Liste **Funktionsgruppe** auf **Andere**.

   c Wählen Sie den Ergebnistyp MQM aus, und klicken Sie dann auf **Weiter**.

3 Wählen Sie das Abfrage-Layout aus.

   a Wählen Sie im Menü **Ergebnisse anzeigen als** das Layout aus.

   b Konfigurieren Sie die übrigen Layout-Optionen, und klicken Sie dann auf **Weiter**

   c Wählen Sie auf der Seite **Filter** die Eigenschaften und Operatoren aus, mit denen die Abfragedaten beschränkt werden.

4 Wählen Sie die Abfragespalten aus.

   a Wählen Sie im Menü **Verfügbare Spalten** die Spalten aus, die auf die Abfrage angewendet werden sollen.

   b Wählen Sie im Konfigurationsbereich **Ausgewählte Spalten** die einzelnen Spaltendatentypen aus, und positionieren Sie sie durch Ziehen.

   c Klicken Sie auf **Weiter**.

5 Wählen Sie im Menü **Verfügbare Eigenschaften** die Eigenschaften aus, und konfigurieren Sie die entsprechenden Werte.

6 Klicken Sie auf **Ausführen**.

7 Speichern Sie die Abfrage.

   a Klicken Sie auf **Speichern**.

   b Geben Sie auf der Seite **Abfrage speichern** den Namen der Abfrage ein, fügen Sie ggf. Anmerkungen hinzu, und wählen Sie dann die Gruppe aus.

   c Klicken Sie auf **Speichern**.

Deinstallieren von McAfee Quarantine Manager mit ePolicy Orchestrator

Entfernen Sie das McAfee Quarantine Manager-Paket und die Erweiterungen sowie die Komponente MySQL for McAfee Quarantine Manager von den Client-Computern und aus dem ePolicy Orchestrator-Repository.

Aufgaben

- *Entfernen von MQM von Client-Computern* auf Seite 35
  Verwenden Sie McAfee ePO, um MQM von Client-Computern zu entfernen.
- *Entfernen der Pakete* auf Seite 35
  Sie können die McAfee Quarantine Manager-Pakete von McAfee ePO aus deinstallieren.
- *Entfernen der Erweiterungen* auf Seite 36
  Sie können die Erweiterungen von McAfee ePO aus deinstallieren.

Entfernen von MQM von Client-Computern

Verwenden Sie McAfee ePO, um MQM von Client-Computern zu entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** (Systemlisten | SSO-Katalog).
3. Wählen Sie zunächst das System und dann **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern** aus.
4. Wählen Sie **Aktionen** | **Neuer Task** aus.
5. Fügen Sie auf der Seite **Generator für Client-Tasks** einen Namen und Anmerkungen ein, wählen Sie in der Dropdown-Liste **Typ**den Eintrag **Produktausbringung** aus, und klicken Sie dann auf **Weiter**.
6. Nehmen Sie unter **Konfiguration** die erforderlichen Einstellungen vor, und klicken Sie dann auf **Weiter**.
   a. Wählen Sie unter **Zielplattformen** die Plattform **Windows** aus.
   b. Wählen Sie unter **Produkte und Komponenten** das Produkt **McAfee Quarantine Manager 7.1.x.x** aus.
   c. Wählen Sie als **Aktion** den Vorgang **Entfernen** aus.
   d. Wählen Sie die Sprache aus.
   e. Wenn Sie nur einen einzelnen Client-Computer entfernen, deaktivieren Sie die Option **Bei jeder Richtlinienerzwingung ausführen (nur Windows)**.
7. Klicken Sie auf **Weiter**, um eine Übersicht des Tasks anzuzeigen, und klicken Sie dann auf **Speichern**.
8. Senden Sie einen Aufruf zur Agentenreaktivierung.

Entfernen der Pakete

Sie können die McAfee Quarantine Manager-Pakete von McAfee ePO aus deinstallieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Wählen Sie **Menü** | **Software** | **Master-Repository** aus.
3. Klicken Sie neben **McAfee Quarantine Manager** auf **Löschen**.
4. Wenn Sie das **MySQL for McAfee Quarantine Manager**-Paket entfernen möchten, wiederholen Sie die Schritte 1 und 2, und klicken Sie dann auf den Link „Löschen" für **MySQL for McAfee Quarantine Manager**.

Entfernen der Erweiterungen

Sie können die Erweiterungen von McAfee ePO aus deinstallieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim McAfee ePO-Server als Administrator an.
2. Klicken Sie auf **Menü** | **Software** | **Erweiterungen** für diese Domäne konfiguriert wurde.
3. Entfernen Sie die **McAfee Quarantine Manager**-Erweiterungsdatei.
   a. Klicken Sie im linken Fensterbereich auf **McAfee** | **McAfee Quarantine Manager** für diese Domäne konfiguriert wurde.
   b. Wählen Sie die **McAfee Quarantine Manager**-Erweiterungsdatei aus, und klicken Sie dann auf **Entfernen**.
   c. Wählen Sie **Erzwungenes Entfernen. Alle Prüfungen oder Fehler werden umgangen.** aus, und klicken Sie dann auf **OK**.
4. Entfernen Sie die McAfee Quarantine Manager-Berichtserweiterungsdatei.
   a. Klicken Sie im linken Fensterbereich auf **McAfee** | **McAfee Quarantine Manager** für diese Domäne konfiguriert wurde.
   b. Wählen Sie die McAfee Quarantine Manager-Berichtserweiterungsdatei aus, und klicken Sie dann auf **Entfernen**.
   c. Wählen Sie **Erzwungenes Entfernen. Alle Prüfungen oder Fehler werden umgangen.** aus, und klicken Sie dann auf **OK**.
5. Entfernen Sie die McAfee Quarantine Manager-Hilfeerweiterungsdatei.
   a. Klicken Sie im linken Fensterbereich auf **McAfee** | **Hilfe** für diese Domäne konfiguriert wurde.
   b. Wählen Sie die McAfee Quarantine Manager-Hilfeerweiterungsdatei aus, und klicken Sie dann auf **Entfernen**.
   c. Wählen Sie **Erzwungenes Entfernen. Alle Prüfungen oder Fehler werden umgangen.** aus, und klicken Sie dann auf **OK**.

5 Arbeitsschritte nach der Installation

Führen Sie die Erstkonfiguration der Datenbank durch, und testen Sie dann die Installation.

Inhalt

- *Konfigurieren der Datenbank*
- *Testen der Installation*
- *Erneutes Branding von McAfee Quarantine Manager*

Konfigurieren der Datenbank

Konfigurieren Sie eine unterstützte externe Datenbank, und überprüfen Sie, ob McAfee Quarantine Manager eine Verbindung mit dieser Datenbank herstellen kann.

Vorgehensweise

1 Klicken Sie auf **Start** | **Programme** | **McAfee** | **Quarantäne-Manager** | **DB Management-UI** (Systemlisten | SSO-Katalog).

> Sie können auch auf der Anmeldeseite für Administratoren auf **Datenbank konfigurieren** klicken und die Anmeldeinformationen für den Systemadministrator eingeben.

2 Konfigurieren Sie die Optionen auf der Seite **Datenbankkonfiguration**.

a Geben Sie im Feld **Datenbanktyp** den Datenbanktyp ein.

b Geben Sie im Feld **Datenbank-Server** die IP-Adresse oder den Host-Namen des Datenbank-Servers ein.

> Geben Sie für SQL Server benannte Instanzen in folgendem Format ein: `Server\BenannteInstanz`.

c Geben Sie im Feld **Benutzername** den Namen des Datenbankbenutzers ein, anhand dessen McAfee Quarantine Manager eine Verbindung mit dem Datenbank-Server herstellt. Der Benutzername muss über Schreibzugriff auf die unter **Datenbankname** definierte Datenbank verfügen.

d Geben Sie im Feld **Kennwort** das Kennwort ein.

e Geben Sie im Feld **Datenbankname** den Namen der Datenbank ein.

f Geben Sie im Feld **Datenbank-Port** die Port-Nummer ein, unter der McAfee Quarantine Manager eine Verbindung mit dem Datenbank-Server herstellt.

g Wenn Verbindungen mit der Datenbank über den Standard-Port hergestellt werden sollen, wählen Sie **Standard-Port verwenden** aus.

h Wenn Sie alle Daten aus der Datenbank löschen und ein Datenbankschema erstellen möchten, wählen Sie **Quarantine Manager-Schema erstellen** aus, und geben Sie anschließend die E-Mail-Adresse und das Kennwort ein.

Das *Schema* ist die Struktur der Datenbank, die die Objekte in der Datenbank definiert. Dies umfasst die Tabellen, Felder, Indizes und Prozeduren.

3 Klicken Sie auf **Testen**.

Daraufhin öffnet sich ein Dialogfeld mit der Meldung, dass die Datenbank erfolgreich konfiguriert wurde.

4 Klicken Sie zum Speichern der Einstellungen der Datenbankkonfiguration auf **Übernehmen**.

5 Wählen Sie zum Erstellen eines McAfee Quarantine Manager-Schemas **Quarantine Manager-Schema erstellen** aus.

Testen der Installation

Sie können die Verbindung zwischen McAfee Quarantine Manager und anderen McAfee-Produkten überprüfen.

- Wenn Sie McAfee Quarantine Manager mit der McAfee Email and Web Security Appliance oder McAfee Email Gateway konfigurieren, müssen Sie die Option **Off-Box-McAfee Quarantine Manager (MQM)-Dienst verwenden** aktivieren.
- Wenn Sie McAfee Quarantine Manager mit McAfee Security for Microsoft Exchange konfigurieren, vergewissern Sie sich auf der Seite **Einstellungen und Diagnosen** | **Erkannte Elemente**, dass die McAfee Quarantine Manager-Option aktiviert ist.
- Senden Sie nach der Konfiguration des McAfee-Produkts mit McAfee Quarantine Manager einige Test-E-Mails mit bösartigem Inhalt an das verbundene McAfee-Produkt.

Vorgehensweise

1 Wählen Sie nach der Installation von McAfee Quarantine Manager **Start** | **Programme** | **McAfee** | **Quarantäne-Manager** | **Administrator-UI** aus.

2 Melden Sie sich mit dem Super-Administratorkonto an, das Sie während der Installation der Software festgelegt haben. Sie müssen sich erfolgreich anmelden können.

3 Klicken Sie auf **Dashboard**.

4 Klicken Sie unter **Verbundene McAfee-Produkte** auf **Testen**, um die Verbindung zwischen der Software und dem McAfee-Produkt zu überprüfen.

Wenn die Option **Verwenden Sie HTTP für die Kommunikation mit dem MQM-Server (MQM v6 und höher)** in McAfee Email and Web Security Appliance aktiviert ist, kann die Verbindung nicht durch **Testen** überprüft werden.

5 Wählen Sie **Admin-Verwaltung** | **Domänen verwalten** aus. Geben Sie den **Domänennamen** ein, und klicken Sie dann auf **Hinzufügen**, um eine Domäne zum Speichern der domänenbasierten isolierten Objekte zu erstellen.

Wenn beispielsweise Objekte für die Domäne „xyz.com" isoliert werden sollen, erstellen Sie einen Domänennamen mit „@xyz.com", und klicken Sie dann auf **Hinzufügen**.

6 Wählen Sie **Quarantäne-Management** | **Isolierte Elemente** aus. Elemente, die vom unterstützten McAfee-Produkt isoliert wurden, sind im Bereich **Ergebnisse anzeigen** aufgeführt.

7 Klicken Sie auf der Benutzeroberfläche für Administratoren auf **Isolierte Objekte**, und wählen Sie den Domänennamen aus der Dropdown-Liste aus, um die isolierten E-Mails für die erstellte Domäne anzuzeigen.

Erneutes Branding von McAfee Quarantine Manager

Mit dem Kit für erneutes Branding von McAfee Quarantine Manager können Sie verschiedene Komponenten der Administrator- und der Benutzeransicht von McAfee Quarantine Manager entsprechend dem Design und den Slogans Ihres Unternehmens gestalten.

Siehe auch

Anpassen der McAfee Quarantine Manager-Software an das Erscheinungsbild Ihres Unternehmens auf Seite 105

Konfiguration und Verwendung

Sie können Domänen und Server einrichten und festlegen, wie die Quarantäne-Einstellungen der Benutzer und Übermittlungen durch Benutzer behandelt bzw. verarbeitet werden sollen.

Kapitel 6 *Server-Verwaltung*
Kapitel 7 *Domänenverwaltung*
Kapitel 8 *Verwalten von Benutzerkonten*
Kapitel 9 *Verwalten isolierter Elemente*
Kapitel 10 *Verwalten von Tasks*
Kapitel 11 *Übermittlungen durch Benutzer*
Kapitel 12 *Benutzerinteraktionen*

6 Server-Verwaltung

Sie können Administratorkonten erstellen und diese den Domänen zuweisen, die für den McAfee Quarantine Manager-Server verantwortlich sind.

Inhalt

- *Administratortypen*
- *Authentifizierungsmodi*
- *Verwenden von LDAP-Gruppen als McAfee Quarantine Manager-Administratoren*
- *Erstellen von Administratoren mit eingeschränkten Berechtigungen*

Administratortypen

McAfee Quarantine Manager unterstützt mehrere Typen von Administratorkonten, die Sie konfigurieren und verwalten können. Diese Kontotypen verfügen über jeweils unterschiedliche Rechte und Berechtigungen.

Tabelle 6-1 Typen von Administratorkonten

Administratortyp	Berechtigungen
Super-Administrator	• Wird während der Installation von McAfee Quarantine Manager erstellt. • Kann weitere Administratoren erstellen. • Verfügt über sämtliche Rechte und Berechtigungen und vollständige Kontrolle über das Produkt.
Super-Administrator-Alias	• Ist gleichrangig mit dem Super-Administrator. • Kann keinen anderen Super-Administrator-Alias erstellen.
Domänenadministrator	• Kann Domänen unabhängig verwalten. • Verfügt über die vom Super-Administrator festgelegten Rechte und Berechtigungen.
Domänenadministrator-Alias	• Ist gleichrangig mit dem Domänenadministrator. • Kann keinen anderen Domänenadministrator-Alias erstellen.
Operator	Verfügt über die gleichen Rechte und Berechtigungen wie der Super-Administrator mit folgenden Ausnahmen: • Anzeigen des Nachrichtentexts isolierter E-Mails, • Herunterladen bzw. Weiterleiten isolierter Elemente, • Bearbeiten der Administratorauthentifizierung.

Authentifizierungsmodi

Für Administratoren sind unterschiedliche Authentifizierungsmodi verfügbar.

- **Verzeichnis-Server-Gruppen**: Authentifiziert LDAP-Gruppen als Administratoren. Wenn Sie LDAP-Gruppen Administratorrechte zuweisen, werden allen Benutzern in den jeweiligen LDAP-Gruppen automatisch Administratorrechte zugewiesen.
- **Quarantine Manager-Konten**: Administratoren werden auf dem McAfee Quarantine Manager-Server authentifiziert. Die Speicherung der Administrator-Anmeldeinformationen und die Authentifizierung erfolgen auf dem McAfee Quarantine Manager-Server.
- **Single-Sign-On über HTTP-Header**: Es wird ein HTTP-Header als Anmelde-ID verwendet.

Der Modus **Single-Sign-On über HTTP-Header** kommt zur Anwendung, wenn die Authentifizierung auf einem externen Server ausgeführt wird. Der externe Server leitet die Anfrage an McAfee Quarantine Manager weiter.

Sie können den Modus für die Administratorauthentifizierung wechseln. Beim Wechsel zu einem anderen Authentifizierungsmodus werden die vorherige Authentifizierung und die vorherigen Zuordnungen von Administratoren zu Domänen ungültig. Darüber hinaus müssen Sie das Super-Administratorkonto für die neue Authentifizierung konfigurieren.

Angenommen, McAfee Quarantine Manager verwaltet die beiden Domänen „abc.com" und „xyz.com", und als Authentifizierungsmodus ist **Quarantine Manager-Konten** eingestellt. Zudem sind Sie der Super-Administrator mit der ID „super@mqm.com" und haben beide Domänen dem Domänenadministrator „d1@mqm.com" zugewiesen.

Wenn Sie in einen anderen Authentifizierungsmodus wechseln, beispielsweise zu LDAP, werden alle Administratorkonten und Domänenzuordnungen ungültig.

Wenn Sie neue Administratoren erstellen und unter der neuen Authentifizierung Domänen zuweisen, bleibt die Administratorkonfiguration unter **Quarantine Manager-Konten** deaktiviert. Die Administratoren und Domänen verbleiben auf dem Server.

Verwenden von LDAP-Gruppen als McAfee Quarantine Manager-Administratoren

Sie können Benutzer, die zu LDAP-Gruppen gehören, als Administratoren festlegen.

Diese Gruppen werden auf dem LDAP-Server definiert. Wenn Gruppen auf dem LDAP-Server als Administratoren festgelegt sind, kann jeder Benutzer, der Mitglied der betreffenden Gruppe ist, als Administrator fungieren.

Sie können Benutzern in LDAP-Gruppen ermöglichen, als Administratoren zu fungieren.

- Der LDAP-Server wird unter **Einstellungen und Diagnose** | **Kommunikation** konfiguriert.
- In McAfee Quarantine Manager kann jedoch nicht eingestellt werden, dass untergeordnete LDAP-Gruppen als Administratoren fungieren.
- Melden Sie sich für Active Directory beim Computer als der Gruppenmitglied-Benutzer an, der als Administrator fungieren soll.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche für Administratoren von McAfee Quarantine Manager mit dem Konto des Super-Administrators an, das Sie während der Installation angegeben haben.

2 Klicken Sie auf **Administratorverwaltung** | **Administrator verwalten** | **Administrator-Authentifizierung** (Systemlisten | SSO-Katalog).

3 Wählen Sie **Verzeichnis-Server-Gruppen** aus, und klicken Sie auf **Weiter**.

Daraufhin wird eine Liste der registrierten LDAP-Gruppen angezeigt.

4 Wählen Sie die Gruppe aus.

5 Bestätigen Sie die Auswahl bei einer entsprechenden Aufforderung, indem Sie auf **Ja** klicken.

Die Einstellungen für die Administratorauthentifizierung werden geändert, und Sie werden abgemeldet.

6 Wählen Sie zum Anmelden mit den neuen Anmeldeinformationen **Klicken Sie hier** aus.

- Geben Sie für alle LDAP-Gruppen mit Ausnahme von Active Directory die Anmeldeinformationen an.
- Für Active Directory melden Sie sich automatisch mit dem derzeit verwendeten Windows-Konto an.

- Super-Administratoren können LDAP-Gruppen zuweisen, die als Operatoren und Domänenadministratoren fungieren.
- Die Alias-Rolle kann für die Verzeichnis-Server-Authentifizierung nicht verwendet werden.

Erstellen von Administratoren mit eingeschränkten Berechtigungen

Erstellen Sie Super-Administrator- und Domänenadministratorkonten, und weisen Sie Administratorrechte zu.

Vorgehensweise

1 Melden Sie sich mit dem Super-Administratorkonto bei der Benutzeroberfläche für Administratoren von McAfee Quarantine Manager an.

2 Klicken Sie auf **Administratorverwaltung** | **Administrator verwalten** | **Neues Konto hinzufügen** (Systemlisten | SSO-Katalog).

3 Wählen Sie auf der Seite **Kontorolle und Details** in der Liste **Kontorolle** den Eintrag **Domänenadministrator** aus, und geben Sie anschließend die Informationen für die **Kontodetails** ein.

a Geben Sie im Feld **Kontoname** den Administratornamen ein.

b Geben Sie im Feld **Konto-E-Mail** die Administrator-E-Mail-Adresse ein, die Sie bei zur der Anmeldung bei der Benutzeroberfläche angegeben haben.

McAfee Quarantine Manager sendet eine E-Mail-Benachrichtigung an den Administrator, wenn ein SMTP-Server für die Domäne konfiguriert wurde.

c Geben Sie das Kontokennwort ein, und bestätigen Sie es.

Wenn Sie auf **Fertig stellen** klicken, wird das Domänenadministratorkonto mit Zugriff auf alle Quarantäne-Warteschlangen und mit vollständigen Verwaltungsrechten erstellt.

4 Klicken Sie zum Anzeigen des Abschnitts **Sichtbare Quarantäne-Warteschlangen** auf **Weiter**.

5 Wenn Sie den Zugriff auf alle Arten von isolierten Elementen gestatten möchten, wählen Sie **Alle Warteschlangen** aus.

Sie können eine übergeordnete Kategorie auswählen, um alle untergeordneten Warteschlangen einzuschließen. Wenn Sie die Zugriffsberechtigung für bestimmte Warteschlangen erteilen möchten, wählen Sie die gewünschten Warteschlangen aus, und klicken Sie auf **Weiter**.

Wenn Sie auf **Fertig stellen** klicken, wird das Domänenadministratorkonto mit vollständigen Verwaltungsrechten erstellt.

6 Weisen Sie unter **Management-Berechtigungen** Administratorrechte zu.

Wenn Sie dem Domänenadministrator alle Berechtigungen gewähren möchten, wählen Sie **Alle Berechtigungen** aus.

Sie können nur ausgewählte Berechtigungen gewähren, indem Sie die Berechtigungen deaktivieren, die dem Administrator nicht zugewiesen werden sollen. Sie können auch die Rechte innerhalb einer Kategorie deaktivieren.

Standardmäßig sind alle Berechtigungen aktiviert.

7 Klicken Sie zum Abschließen der Zuweisung von Rechten und Berechtigungen für den Domänenadministrator auf **Fertig stellen**.

Wenn einem Domänenadministrator bestimmte Rechte oder Berechtigungen nicht gewährt werden, sind die irrelevanten Optionen für den betreffenden Domänenadministrator in der Benutzeroberfläche ausgeblendet. Wenn beispielsweise dem Domänenadministrator die Berechtigung **Berichte generieren** nicht gewährt wurde, wird für diesen Folgendes nicht angezeigt:

- Link **Grafische Berichte**
- Registerkarte **Berichte** im **Dashboard**

7 Domänenverwaltung

Die Domänenverwaltung umfasst u. a. das Hinzufügen und Importieren von Domänen zu McAfee Quarantine Manager sowie das Exportieren von Domänen aus McAfee Quarantine Manager, das Zuordnen von Domänen, das Ändern der Konfigurationen sowie das Zuordnen von Gruppen aus verbundenen McAfee-Produkten.

Inhalt

- *Hinzufügen oder Importieren von Domänen zu McAfee Quarantine Manager*
- *Zuweisen von Domänen zu Domänenadministratoren*
- *Ändern von Domänenkonfigurationen*
- *Ändern mehrerer Domänenkonfigurationen*
- *Erstellen einer Zuordnung zwischen Domänen und Gruppen in verbundenen McAfee-Produkten*

Hinzufügen oder Importieren von Domänen zu McAfee Quarantine Manager

Wenn Sie Elemente gemäß den erstellten Domänen isolieren, können Sie später isolierte Elemente aus einer bestimmten Domäne suchen und anzeigen.

Für verschiedene Funktionen in McAfee Quarantine Manager ist es zwingend erforderlich, dass alle vom Unternehmen verwalteten E-Mail-Domänen hinzugefügt werden. Dies gilt beispielsweise für E-Mail-Digests und Benutzerzugriff. Im Abschnitt **Domänen verwalten** können Sie Folgendes durchführen:

- Hinzufügen einer Domäne oder Ändern einer Domänenkonfiguration,
- Importieren mehrerer Domänen aus einer CSV-Datei,
- Auswählen und Zuweisen von Domänenadministratoren,
- Löschen von Domänen.

Wenn die Domäne nicht registriert ist und ein Element isoliert wird, wird es unter **Andere** eingeordnet.

Aufgaben

- *Hinzufügen von Domänen* auf Seite 48
  Sie Domänen hinzufügen, die in McAfee Quarantine Manager verwaltet werden sollen.
- *Gleichzeitiges Importieren mehrerer Domänen* auf Seite 48
  Sie können mehrere Domänen mithilfe einer CSV- oder TXT-Datei auf einmal importieren. In einer CSV-Datei werden die Domänennamen in einer Spalte angezeigt.
- *Exportieren von Domänen* auf Seite 48
  Sie können alle in McAfee Quarantine Manager registrierten Domänen an einen zuvor festgelegten Speicherort exportieren.

Hinzufügen von Domänen

Sie Domänen hinzufügen, die in McAfee Quarantine Manager verwaltet werden sollen.

Vorgehensweise

1 Melden Sie sich mit einem Super-Administrator- oder Operatorkonto an.

2 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** | **Domäne hinzufügen** aus.

3 Geben Sie im Feld **Domänenname** den Domänennamen ein, und klicken Sie anschließend auf **Hinzufügen**.

- Der Domänenname darf aus höchstens 61 Zeichen bestehen und darf Buchstaben, Zahlen und Punkte enthalten.
- McAfee Quarantine Manager unterstützt keine Platzhalter, und Subdomänen werden explizit registriert.

Die Domäne wird nun in der **Liste der verwalteten Domänen** aufgeführt.

Gleichzeitiges Importieren mehrerer Domänen

Sie können mehrere Domänen mithilfe einer CSV- oder TXT-Datei auf einmal importieren. In einer CSV-Datei werden die Domänennamen in einer Spalte angezeigt.

Vorgehensweise

1 Melden Sie sich mit einem Super-Administrator- oder Operatorkonto an.

2 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** | **Domänen importieren/exportieren** aus.

3 Geben Sie zum Auswählen der gewünschten Datei entweder den **Dateipfad** ein, oder klicken Sie auf **Durchsuchen**.

4 Klicken Sie auf **Importieren**.

Nun wird ein Bericht mit Informationen zum erfolgreichen bzw. fehlgeschlagenen Domänenimport erstellt. Die Domäne wird nun in der **Liste der verwalteten Domänen** aufgeführt. Wenn mehrere Domänen importiert wurden, werden nun alle in der CSV-Datei enthaltenen Domänen in der **Liste der verwalteten Domänen** aufgeführt.

Exportieren von Domänen

Sie können alle in McAfee Quarantine Manager registrierten Domänen an einen zuvor festgelegten Speicherort exportieren.

Vorgehensweise

1 Melden Sie sich mit einem Super-Administrator- oder Operatorkonto an.

2 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** | **Domänen importieren/exportieren** aus.

3 Wählen Sie aus der **Liste der verwalteten Domänen** eine oder mehrere Domänen aus, und klicken Sie dann auf **Exportieren**.

Bei Auswahl mehrerer Domänen werden diese zusammen in eine Textdatei exportiert.

4 Wenn Sie diese Domänenliste im Textformat anzeigen möchten, klicken Sie im Fenster **Datei-Download** auf **Öffnen**.

5 Möchten Sie die Textdatei hingegen an einem bestimmten Verzeichnis speichern, dann klicken Sie auf **Speichern**.

6 Wenn Sie zum vorherigen Bildschirm zurückkehren möchten, klicken Sie auf **Abbrechen**.

Zuweisen von Domänen zu Domänenadministratoren

Sie können Administratoren einer Domäne oder mehreren Domänen zuweisen. Erstellen Sie zum Delegieren des Quarantäne-Managements für Domänen einen Domänenadministrator, und weisen Sie die Domänen zu.

Vorgehensweise

1 Melden Sie sich mit einem Super-Administrator- oder Operatorkonto an.

2 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** aus.

3 Wählen Sie in der **Liste der verwalteten Domänen** die Domäne aus, und klicken Sie dann auf **Administrator zuweisen**.

Wenn Sie Domänenadministratoren nur eine Domäne zuweisen möchten, klicken Sie in der Spalte **Domänen-Admin** auf **Zuweisen**.

4 Wählen Sie im Konfigurationsbereich **Admin zuweisen** in der **Administratorenliste** Administratoren aus, und klicken Sie auf **Hinzufügen**.

5 Klicken Sie auf **Zuweisen**.

- Wenn Sie die **Liste der zugewiesenen Administratoren** leer lassen, werden die Domänen vom Super-Administrator verwaltet.
- Wenn eine einzelne Domäne zugewiesen wird, werden die zuvor zugewiesenen Administratoren automatisch in die **Liste der zugewiesenen Administratoren** eingetragen.
- Wenn mehrere Domänen zugewiesen werden, bleibt die **Liste der zugewiesenen Administratoren** leer.

6 Sie können auf **Abbrechen** klicken, um die Änderungen rückgängig zu machen und zum vorherigen Bildschirm zurückzukehren.

Sie können mehrere Domänen auswählen und ihnen einen bestimmten Administrator oder mehrere Administratoren zuweisen. Außerdem können Sie den einer Domäne zugewiesenen Administrator wieder entfernen.

Ändern von Domänenkonfigurationen

Sie können die Benutzer- und IP-Adresseinstellungen für Domänen ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich mit einem Super-Administrator- oder Operatorkonto an.

2 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** aus.

3 Wählen Sie in der **Liste der verwalteten Domänen** die Domäne aus, und klicken Sie dann auf **Konfiguration ändern**.

4 Wählen Sie die **Benutzer- und Warteschlangeneinstellungen** für die einzelnen Erkennungstypen, E-Mail-Server-Parameter und Digest-Einstellungen aus.

5 Legen Sie unter **Mail-Einstellungen** die Parameter für den **E-Mail-Server** fest, um die Kommunikation mit den Benutzern der ausgewählten Domäne zu ermöglichen.

a Geben Sie im Feld **Server-Name/IP-Adresse** den Host-Namen oder die IP-Adresse des E-Mail-Servers für diese Domäne ein.

b Geben Sie im Feld **Port** den E-Mail-Server an.

Standardmäßig wird bei der Einrichtung die Port-Nummer 25 angegeben. Sie können diese Einstellung bei Bedarf ändern.

c Wählen Sie **TLS verwenden** (Transport Layer Security) aus, um den Datenschutz für E-Mails zu verbessern, die an die Benutzer dieser Domäne gesendet werden.

Das TLS-Protokoll schützt die Kommunikation zwischen Client- und Server-Anwendungen über ein Netzwerk vor Manipulation und Abhören. TLS sorgt anhand von Kryptografie für die Authentifizierung der Endgeräte und die Sicherung der Kommunikation über das Internet.

Der SMTP-Server unterstützt immer die SMTP-Erweiterung STARTTLS. Achten Sie darauf, dass sich das entsprechende Zertifikat am erforderlichen Speicherort befindet.

6 Legen Sie unter **Digest-Einstellungen** die Parameter für das Senden von Digest-Nachrichten an Domänenbenutzer durch McAfee Quarantine Manager fest.

7 Auf der Registerkarte **Vorlagen** können Sie vordefinierte Formate für E-Mail-Nachrichten verwenden, die an Benutzer gesendet werden sollen.

a Geben Sie die E-Mail-Adresse des Absenders ein. Die Standard-E-Mail-Adresse des Absenders lautet McAfeeQuarantineManager@McAfee.com. Sie können diese Adresse bei Bedarf ändern.

b Geben Sie im Feld **Betreff** den Betreff der E-Mail ein.

c Wählen Sie im Feld **E-Mail-Format** das Format der zu sendenden E-Mail aus.

d Wenn Sie **HTML-Anlage** auswählen, wählen Sie im Feld **Formularmethode** die Option **Post** oder **Get** aus.

Ändern mehrerer Domänenkonfigurationen

Sie können die Konfigurationseinstellungen für mehrere Domänen ändern.

Vorgehensweise

1 Wählen Sie **Administratorverwaltung** | **Domänen verwalten** aus

2 Wählen Sie in der **Liste der verwalteten Domänen** die zu ändernden Domänen aus, und klicken Sie dann auf **Konfiguration ändern**.

3 Wählen Sie die **Benutzer- und Warteschlangeneinstellungen** für die einzelnen Erkennungstypen, E-Mail-Server-Parameter und Digest-Einstellungen aus.

Während der Bearbeitung der Vorlagen mehrerer Domänen sind alle Werte auf der Registerkarte **Vorlagen** leer. Nur die geänderten Einstellungen werden auf die ausgewählten Domänen angewendet.

Erstellen einer Zuordnung zwischen Domänen und Gruppen in verbundenen McAfee-Produkten

Sie können Gruppen, die in verbundenen McAfee-Produkten registriert sind, einer Domäne zuweisen.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Administratorverwaltung** | **Domänen verwalten** für diese Domäne konfiguriert wurde.

2 Wählen Sie in der **Liste der verwalteten Domänen** eine Domäne aus, und klicken Sie dann auf **Ändern/ Anzeigen**.

3 Wählen Sie im Konfigurationsbereich **Gruppen zuweisen** in der **Gruppenliste** eine oder mehrere Gruppen aus, und klicken Sie dann auf **Hinzufügen**.

4 Klicken Sie auf **Zuweisen**.

- Die Administratoren, die die Domäne verwalten, können Blacklists und Whitelists für die zugewiesenen Gruppen verwalten.
- Wenn Sie auf **Entfernen** klicken, wird die Gruppe dem Super-Administrator zugewiesen.
- Wenn Sie auf **Abbrechen** klicken, werden alle Änderungen verworfen, und Sie kehren zu **Domänen verwalten** zurück.

8 Verwalten von Benutzerkonten

Die Benutzerkontenverwaltung in McAfee Quarantine Manager umfasst das Erstellen, Importieren, Registrieren und Ändern der Benutzerkonten. Sie können auch auf dem LDAP-Server definierte Benutzerkonten verwalten.

Inhalt

- *Erstellen von Benutzerkonten*
- *Importieren von Benutzern über LDAP*
- *Importieren von Benutzern anhand einer CSV- oder TXT-Datei*
- *Importieren von Benutzern anhand einer XML-Datei*
- *Automatisches Registrieren von Benutzern*
- *Ändern der Benutzerkonfiguration*
- *Registrieren einer Verteilerliste*

Erstellen von Benutzerkonten

Sie können in McAfee Quarantine Manager Benutzerkonten erstellen.

Vorgehensweise

1. Klicken Sie auf **Start** | **Programme** | **McAfee** | **Quarantine Manager** | **Benutzer-UI** (Systemlisten | SSO-Katalog).
2. Klicken Sie auf **Neuer Benutzer? Zum Registrieren hier klicken.**
3. Geben Sie im Feld **E-Mail-Adresse** die zu der von McAfee Quarantine Manager verwalteten Domäne gehörige E-Mail-Adresse ein.
4. Klicken Sie auf **Registrieren.**

Der Benutzer wird nun erstellt, und es wird eine E-Mail an die E-Mail-Adresse gesendet, die Sie bei der Registrierung mit Ihren Anmeldeinformationen angegeben haben. Der Benutzername wird nun auf dem Bildschirm **Benutzerverwaltung** unter **Endbenutzerverwaltung** | **Kontoverwaltung** aufgeführt.

Importieren von Benutzern über LDAP

Sie können Benutzer, die auf einem LDAP-Server registriert sind, in McAfee Quarantine Manager importieren.

> **Bevor Sie beginnen**
>
> Achten Sie darauf, dass der Autorisierungsmodus **LDAP-Server-Konten** eingestellt ist.

Wenn Sie eine Verbindung mit einem LDAP-Server konfigurieren und herstellen, erleichtert dies die Benutzerauthentifizierung und -synchronisierung und die Erweiterung von Verteilerlisten.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Einstellungen und Diagnose** | **Kommunikation** | **LDAP-Server** für diese Domäne konfiguriert wurde.

Für jeden LDAP-Server-Typ müssen Parameter festgelegt werden, um die Kommunikation mit dem McAfee Quarantine Manager-Server zu ermöglichen.

2 Wählen Sie in der Dropdown-Liste **Server-Typ** den Server-Typ aus.

3 Überprüfen Sie die Verbindung, indem Sie auf **Testen** klicken.

Wenn Sie den auf einem LDAP-Server vorhandenen Benutzern Administratorberechtigungen zuweisen möchten, können Sie hierfür die auf dem McAfee Quarantine Manager-LDAP-Server befindliche Benutzerliste synchronisieren.

4 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Endbenutzerverwaltung** | **Allgemein** für diese Domäne konfiguriert wurde.

5 Konfigurieren Sie die unter **Benutzersynchronisierungseinstellungen** befindlichen Optionen.

- Die Registrierungsbenachrichtigung wird nur dann an Benutzer gesendet, wenn die Domäne über einen gültigen SMTP-Server verfügt, der unter **Einstellungen und Diagnose** | **Kommunikation** konfiguriert wurde.
- Wenn Sie den Inhalt der E-Mail zur Benutzerregistrierung anpassen möchten, wählen Sie **Administratorverwaltung** | **Domänenverwaltung** | **Ihre Domäne** | **Konfiguration ändern** | **Vorlagen** aus.

6 Erstellen Sie einen Benutzersynchronisierungs-Task, um Benutzer vom LDAP-Server zu importieren.

Siehe auch

Automatisches Synchronisieren und Registrieren von Benutzerlisten auf Seite 62

Importieren von Benutzern anhand einer CSV- oder TXT-Datei

Sie können mehrere Benutzer auf einmal registrieren, indem Sie eine Textdatei importieren, die eine Liste der entsprechenden Benutzer (durch Trennzeichen voneinander getrennt) enthält. Es werden das CSV- und das TXT-Dateiformat unterstützt.

Es werden nur Benutzer von Domänen hinzugefügt, die in McAfee Quarantine Manager registriert sind. Wählen Sie zum Hinzufügen von Domänen **Administratorverwaltung** | **Domänen verwalten** aus.

Vorgehensweise

1 Wählen Sie im Hauptmenü von McAfee Quarantine Manager **Endbenutzerverwaltung** | **Benutzerverwaltung** | **Allgemein** aus.

2 Konfigurieren Sie die für den **Benutzerimport** verfügbaren Einstellungen.

a Klicken Sie zum Auswählen der zu importierenden Benutzerlistendatei auf **Durchsuchen**.

b Wenn die zu importierende Datei eine Header-Zeile (Überschrift) enthält, aktivieren Sie die Option **Eingabedatei enthält Header**.

c Wählen Sie in der Dropdown-Liste **Spaltentrennzeichen** das gewünschte Zeichen aus.

Das entsprechende Trennzeichen darf nicht in den zu importierenden E-Mail-Adressen enthalten sein.

d Geben Sie im Feld **Nummer der Spalte mit Benutzerliste** die Nummer der Spalte ein, in der sich die E-Mail-Adressen der Benutzer befinden.

e Wenn erfolgreich registrierte Benutzer über die Registrierung informiert werden sollen, aktivieren Sie die Option **Registrierungsbenachrichtigungen senden**.

Die Benachrichtigungen werden nur dann an Benutzer gesendet, wenn die Domäne über einen gültigen SMTP-Server verfügt, der unter **Einstellungen und Diagnose** | **Kommunikation** für diese Domäne konfiguriert wurde.

f Wenn Sie den Inhalt der E-Mail zur Benutzerregistrierung anpassen möchten, wählen Sie **Administratorverwaltung** | **Domänenverwaltung** | **Ihre Domäne** | **Konfiguration ändern** | **Vorlagen** aus.

3 Klicken Sie zum Importieren der Benutzerliste und zum Erstellen der Konten auf **Benutzer erstellen**.

Multi-Byte-Zeichen, wie z. B. in Arthur'_brown@63-250-236-237-microsoft.com, werden nur unterstützt, wenn die zu importierende Datei im UTF-8-Format vorliegt.

Importieren von Benutzern anhand einer XML-Datei

Mit der Importfunktion Blacklists und Whitelists können Sie Benutzer und die zugehörigen Konfigurationseinstellungen importieren.

Es werden nur Benutzer von Domänen hinzugefügt, die in McAfee Quarantine Manager registriert sind. Wählen Sie zum Hinzufügen von Domänen **Administratorverwaltung** | **Domänen verwalten** aus.

Vorgehensweise

1 Wählen Sie im Hauptmenü von McAfee Quarantine Manager **Blacklists und Whitelists** | **Importieren und exportieren** aus.

2 Klicken Sie im Konfigurationsbereich **Importieren** auf **Durchsuchen**, und navigieren Sie zu der Konfigurationsdatei, die die zu importierende Benutzerkonfiguration enthält.

3 Wählen Sie zum Zusammenführen der neu importierten Konfiguration mit der früheren Benutzerkonfiguration die Option **Benutzerkonfiguration zusammenführen** aus.

Wenn diese Option deaktiviert ist, wird die Benutzerkonfiguration überschrieben.

4 Klicken Sie auf **Konfiguration importieren**.

Automatisches Registrieren von Benutzern

Sie können anhand bestimmter Einstellungen festlegen, dass Benutzer anhand der Informationen in der Quarantäne-Datenbank automatisch registriert werden.

Vorgehensweise

1 Wählen Sie im Hauptmenü von McAfee Quarantine Manager **Administratorverwaltung** | **Domänen verwalten** und dann die Domäne aus.

2 Klicken Sie auf **Konfiguration ändern**.

3 Wählen Sie auf der Registerkarte **Allgemein** die Option **Endbenutzer während des E-Mail-Digest-Task automatisch anhand der Quarantänedatenbank registrieren** aus.

Wenn diese Funktion in McAfee Quarantine Manager aktiviert ist, ist auch die entsprechende Funktion **Empfängerprüfungen** in den mit McAfee Quarantine Manager verbundenen Produkten aktiviert.

Bei Verwendung dieser Parameter ergeben sich vier mögliche Szenarien.

- Sie wählen nur die Option **Endbenutzer während des E-Mail-Digest-Tasks automatisch anhand der Quarantänedatenbank registrieren** aus:
  - Der Benutzer wird automatisch im Rahmen einer geplanten Digest-Aktivität registriert.
  - An die E-Mail-Adresse des Benutzers wird eine Digest-E-Mail gesendet.
- Sie wählen die Optionen **Bestätigungs-E-Mail senden, bevor Digest-E-Mail gesendet wird** und **Endbenutzer während des E-Mail-Digest-Tasks automatisch anhand der Quarantänedatenbank registrieren** aus:
  - An den Benutzer wird eine Bestätigungs-E-Mail mit einem Registrierungs-Link gesendet.
  - Nachdem der Benutzer auf diesen Link geklickt und die E-Mail Adresse bestätigt hat, wird eine Digest-E-Mail an ihn gesendet.
- Sie wählen die Optionen **Registrierungsbenachrichtigungen senden** und **Endbenutzer während des E-Mail-Digest-Tasks automatisch anhand der Quarantänedatenbank registrieren** aus:
  - Der Benutzer wird automatisch registriert und erhält eine E-Mail mit den Benutzeranmeldeinformationen.
  - Außerdem wird die Digest-E-Mail an die E-Mail-Adresse des Benutzers gesendet.
- Sie wählen alle Optionen aus:
  - Dem Benutzer wird zunächst eine Bestätigungs-E-Mail mit einem Link für die Bestätigung der Benutzer-E-Mail Adresse zugesendet.
  - Nach der entsprechenden Bestätigung erhält der Benutzer eine E-Mail mit den Benutzeranmeldeinformationen.
  - Nach Abschluss des nächsten geplanten Digests erhält der Benutzer dann eine Digest-E-Mail.

4 Klicken Sie auf **Übernehmen**, damit alle vorgenommenen Einstellungen übernommen werden.

5 Wenn Sie die vorherigen Einstellungen wiederherstellen möchten, klicken Sie auf **Abbrechen**.

Ändern der Benutzerkonfiguration

Sie können die Einstellungen für registrierte MQM-Benutzer ändern.

Vorgehensweise

1 Wählen Sie im MQM-Hauptmenü **Endbenutzerverwaltung** | **Benutzerverwaltung** | **Kontoverwaltung** aus.

2 Stellen Sie die Suchoptionen für die Benutzer ein, die Sie ändern möchten.

a Wählen Sie unter **Einschließen** die Benutzerkategorien aus, die bei der Suche berücksichtigt werden sollen.

Sie können in **Kontotyp** mehrere Optionen auswählen. Wählen Sie alle Optionen aus, um nach Benutzern in allen Kategorien zu suchen.

b Wählen Sie den ersten Buchstaben des Benutzerkontos aus, um die Suchfunktion zu verwenden. Wählen Sie beispielsweise **K** aus, um alle Konten zu durchsuchen, die mit „K" beginnen. Klicken Sie auf **Alle**, wenn alle Endbenutzerkonten durchsucht werden sollen.

c Wenn Sie anhand der E-Mail-Adresse eines Benutzers suchen möchten, geben Sie die betreffende Adresse in das Feld **E-Mail-Adresse** ein, und klicken Sie dann auf **Suchen**.

Sie können bei der Suche folgende Platzhalter verwenden:

- `*`: Entspricht einer beliebigen Anzahl von Zeichen
- `?`: Entspricht einem einzelnen Zeichen

3 Wählen Sie den zu ändernden Benutzer aus, und klicken Sie dann auf **Ändern**.

a Geben Sie im Feld **Blacklist** die E-Mail-Adresse des Absenders ein, und klicken Sie dann auf **Hinzufügen**.

b Klicken Sie auf **Whitelist**, geben Sie die E-Mail-Adresse des Absenders ein, und klicken Sie dann auf **Hinzufügen**.

c Klicken Sie auf **E-Mail-Aliasse**, geben Sie im Feld **Name** die E-Mail-Adressen ein, und klicken Sie dann auf **Hinzufügen**.

Diese Optionen werden nur angezeigt, wenn als Authentifizierungsmodus **Quarantine Manager-Konto** ausgewählt ist. Für **LDAP-Server-Konten** sind die E-Mail-Alias-Optionen deaktiviert.

Die Tabelle zeigt den Namen an, unter dem die verfügbaren Alias-Mitglieder des Benutzers aufgelistet sind. Die Spalte **Status** zeigt den aktuellen Status der Alias-E-Mail-Adresse an.

d Klicken Sie auf **Einstellungen**, und legen Sie dann das Kennwort und die Digest-Einstellungen fest.

Wählen Sie zum Anpassen des Inhalts von Digest-E-Mails **Administratorverwaltung** | **Domänenverwaltung** | **Ihre Domäne** | **Konfiguration ändern** | **Vorlagen** aus.

e Klicken Sie auf **E-Mail-Neuzuweisung**, geben Sie die E-Mail-Adresse ein, und klicken Sie dann auf **E-Mails neu zuweisen**.

Wenn die E-Mails weiterhin an den neuen Benutzer umgeleitet werden sollen, wählen Sie **Neuzuweisung speichern** aus. Wenn diese Option nicht ausgewählt wird, werden alle künftig isolierten E-Mails an das vorherige Konto gesendet.

Registrieren einer Verteilerliste

An Verteilerlisten gesendete E-Mails werden von McAfee Quarantine Manager zunächst isoliert. Anschließend erstellt McAfee Quarantine Manager eine Kopie der entsprechenden E-Mail und sendet

diese an jeden in der Verteilerliste enthaltenen Benutzer. Diese können die E-Mail nach dem Empfangen freigeben, löschen oder auf die Blacklist setzen.

Bevor Sie beginnen

Konfigurieren Sie den LDAP-Server unter **Einstellungen und Diagnose** | **Kommunikation** (Systemlisten | SSO-Katalog).

McAfee Quarantine Manager unterstützt keine untergeordneten Verteilerlisten.

Vorgehensweise

1. Wählen Sie in der Dropdown-Liste unter **Server-Typ** den benötigten Server-Typ aus.
2. Wählen Sie **Endbenutzerverwaltung** | **Verteilerliste** | **Verteilerlisten vom LDAP-Server abrufen** aus.
3. Wählen Sie die Verteilerliste aus, und klicken Sie dann auf **Registrieren**.
4. Wählen Sie **Einstellungen und Diagnose** | **Task-Manager** aus.
5. Wenn die in der Verteilerliste registrierten Benutzer zu McAfee Quarantine Manager abgerufen werden sollen, müssen Sie einen **Benutzersynchronisierungs-Task** planen.

9 Verwalten isolierter Elemente

Sie können alle erkannten und isolierten E-Mail-Nachrichten anzeigen, die potenzielle Bedrohungen darstellen. Mithilfe von Filtern können Sie die Suche eingrenzen und nach bestimmten isolierten Elementen suchen, die Ergebnisse anzeigen und die erforderlichen Aktionen ausführen.

Inhalt

- *Suchen nach isolierten Elementen*
- *Durchführen von Aktionen für isolierte Elemente*

Suchen nach isolierten Elementen

Sie können Informationen zu allen E-Mail-Nachrichten mit potenziellen Bedrohungen anzeigen, die entdeckt und isoliert wurden. Mithilfe der Filter können Sie Ihre Suche eingrenzen und die isolierten Elemente mit den zugehörigen Informationen finden.

Es stehen drei Felder für die Auswahl der primären Filter zur Verfügung. Sie können eine Suchoption aus einem Feld oder eine Kombination von Optionen in zwei oder drei Feldern auswählen.

Vorgehensweise

1. Klicken Sie im Administrator-Bildschirm auf **Quarantäne-Management**.
2. Klicken Sie auf der Seite **Isolierte Objekte** auf das Dropdown-Symbol neben einem Feld, und wählen Sie dann bis zu drei Filter aus.
3. Klicken Sie auf **Suchen**.

   Im Raster **Ergebnisse anzeigen** werden nun die isolierten Elemente angezeigt, die Ihren Suchkriterien entsprechen.

Durchführen von Aktionen für isolierte Elemente

Sie können isolierte Elemente für die Freigabe, zum Löschen oder für die Aufnahme in eine Blacklist auswählen. Außerdem stehen noch weitere Aktionen zur Verfügung.

Vorgehensweise

1. Wählen Sie im Raster **Ergebnisse anzeigen** die gewünschten isolierten Elemente aus.
2. Wählen Sie in der Dropdown-Liste **Weitere Aktionen** die gewünschte Option aus, und klicken Sie dann auf **Los**.
3. Klicken Sie zum Freigeben der isolierten E-Mail auf **Freigeben**.

4 Klicken Sie zum Entfernen der isolierten E-Mail auf **Löschen**.

5 Klicken Sie auf **Blacklist**, um die isolierte E-Mail der Blacklist hinzuzufügen.

10 Verwalten von Tasks

Sie können Tasks anzeigen, verwalten und planen.

Tasks sind konfigurierbare Aktionen, die zu einem einstellbaren Zeitpunkt durchgeführt werden. Sie können einen Task für die Ausführung zu einem späteren Zeitpunkt konfigurieren und planen oder einen dringenden Task sofort ausführen.

Bestimmte Tasks müssen regelmäßig durchgeführt werden. Beispielsweise können Sie einen Task planen, der regelmäßig automatisch die MQM bereinigt und alte isolierte Elemente entfernt.

Wenn Sie die LDAP-Authentifizierung verwenden, müssen Sie MQM mit der auf Ihrem LDAP-Server definierten Benutzerliste synchronisieren. Außerdem müssen benutzerbezogen Tasks sofort durchgeführt werden. Dazu zählen beispielsweise:

- Sofortiges Senden einer Quarantäne-Übersicht an einen Benutzer,
- Löschen der von Benutzern isolierten Elemente,
- Absenden einer dringenden E-Mail von MQM an den Benutzer.

Inhalt

- *Konfigurieren einer geplanten Digest-E-Mail*
- *Konfigurieren geplanter Datenbankbereinigungen*
- *Automatisches Synchronisieren und Registrieren von Benutzerlisten*
- *Automatisches Senden von Statusberichten*
- *Synchronisieren von Verteilerlisten*

Konfigurieren einer geplanten Digest-E-Mail

Sie können die Zustellung von Digest-E-Mails an alle Benutzer einrichten, die eine Zusammenfassung aller in einem bestimmten Zeitraum isolierten Elemente mit ausführlichen Informationen zu den isolierten Elementen sowie zu Blacklists und Whitelists enthalten.

Vorgehensweise

1. Wählen Sie in MQM **Einstellungen und Diagnose** | **Task-Manager** | **Geplante Tasks** aus.
2. Wählen Sie unter **Task-Typ** die Option **E-Mail-Digest** aus.
3. Wählen Sie unter **Betroffene Domänen** die Domänen aus. Wenn der E-Mail-Digest an alle Domänenbenutzer gesendet werden soll, wählen Sie **Alle auswählen** aus.
4. Wählen Sie unter **Wann** den Zeitpunkt aus, zu dem der E-Mail-Digest gesendet werden soll.
5. Geben Sie im Feld **Task-Name** den Namen des Tasks ein.

6 Klicken Sie auf **Hinzufügen**, um den Task gemäß den ausgewählten Optionen zu planen.

Daraufhin wird die Meldung **Task wurde hinzugefügt** angezeigt.

7 Klicken Sie zum Bestätigen auf **OK**.

Der E-Mail-Digest-Task wird nun der Liste **Geplante Tasks** hinzugefügt.

Siehe auch

Ändern von Domänenkonfigurationen auf Seite 49

Konfigurieren geplanter Datenbankbereinigungen

Sie können die Datenbank regelmäßig bereinigen. Dabei werden alte Daten, wie zum Beispiel alte Protokolleinträge und isolierte Elemente, gelöscht. Beim Bereinigen der Datenbank wird Speicherplatz freigegeben.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Task-Manager** | **Geplante Tasks** aus.

2 Wählen Sie unter **Task-Typ** die Option **Datenbankbereinigung** aus.

3 Wählen Sie unter **Betroffene Domänen** die Domänen aus. Um die Datenbank von allen in MQM verwalteten Domänenbenutzern zu bereinigen, wählen Sie **Alle auswählen** aus. Um die Datenbank von Domänenbenutzern zu bereinigen, die nicht in MQM verwaltet werden, wählen Sie **Andere** aus.

4 Geben Sie im Feld **Wann** den Zeitpunkt ein, zu dem die Datenbank bereinigt werden soll.

5 Geben Sie im Feld **Task-Name** den Namen des Tasks ein.

6 Klicken Sie auf **Hinzufügen**, um den Task gemäß den ausgewählten Optionen zu planen.

Daraufhin wird die Meldung **Task wurde hinzugefügt** angezeigt.

7 Klicken Sie zum Bestätigen auf **OK**.

Der Datenbankbereinigungs-Task wird nun der Liste **Geplante Tasks** hinzugefügt.

Automatisches Synchronisieren und Registrieren von Benutzerlisten

Sie können die Liste der LDAP-Server-Benutzer synchronisieren und die Benutzer automatisch für MQM registrieren lassen. Außerdem können Sie in den für MQM registrierten LDAP-Verteilerlisten neu hinzugefügte oder geänderte Benutzerkonten synchronisieren.

Wenn Sie die Option **Benutzer löschen, die nicht auf dem LDAP-Server gefunden wurden** auswählen, werden bei Durchführung des folgenden Tasks alle Benutzer gelöscht, die nicht mehr auf dem LDAP-Server vorhanden sind.

Vorgehensweise

1 Wählen Sie in MQM die Optionen **Einstellungen und Diagnose** | **Task-Manager** aus.

2 Wählen Sie unter **Task-Typ** die Option **Benutzersynchronisierung** aus.

3 Geben Sie im Feld **Wann** die Zeiten für die Synchronisierung der Benutzerliste an.

4 Geben Sie im Feld **Task-Name** den Namen des Tasks ein.

5 Klicken Sie zum Bestätigen auf **OK**.

Der Benutzersynchronisierungs-Task wird nun der Liste **Geplante Tasks** hinzugefügt.

Automatisches Senden von Statusberichten

Sie können eine Statusbericht-E-Mail an Administratoren senden, die detaillierte Informationen zu der Datenbankgröße, dem Zählerstatus, den Task-Aktivitäten und den in einem angegebenen Zeitraum aufgetretenen Fehlern enthält.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Task-Manager** | **Geplante Tasks** aus.

2 Wählen Sie unter **Task-Typ** die Option **Status-E-Mail** aus.

3 Wählen Sie unter **Betroffene Domänen** die Domänen aus. An die ausgewählten Domänen wird dann eine Status-E-Mail mit den Quarantäne-Aktivitäten der Domänenbenutzer gesendet. Um den Statusbericht an alle in MQM verwaltete Domänenadministratoren zu senden, wählen Sie **Alle auswählen** aus. Um die Status-E-Mail an Domänenadministratoren zu senden, die nicht in MQM verwaltet werden, wählen Sie **Andere** aus.

4 Wählen Sie im Feld **Wann** den Zeitpunkt aus, zu dem der Task angewendet werden soll.

5 Geben Sie im Feld **Task-Name** den Namen des Tasks ein.

6 Klicken Sie auf **Hinzufügen**, um den Task gemäß den ausgewählten Optionen zu planen.

Daraufhin wird die Meldung **Task wurde hinzugefügt** angezeigt.

7 Klicken Sie zum Bestätigen auf **OK**.

Der Status-E-Mail-Task wird nun in der Liste **Geplante Tasks** angezeigt.

Synchronisieren von Verteilerlisten

Sie können für Verteilerlisten regelmäßige Synchronisierungs-Tasks erstellen.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Task-Manager** | **Geplante Tasks** aus.

2 Wählen Sie unter **Task-Typ** die Option **DL-Synchronisierung** aus.

3 Wählen Sie im Feld **Wann** den Zeitpunkt aus, zu dem der Task angewendet werden soll.

4 Geben Sie im Feld **Task-Name** den Namen des Tasks ein.

5 Klicken Sie auf **Hinzufügen**, um den Task gemäß den ausgewählten Optionen zu planen.

Daraufhin wird die Meldung **Task wurde hinzugefügt** angezeigt.

6 Klicken Sie zum Bestätigen auf **OK**.

Der Task wird nun in der Liste **Geplante Tasks** angezeigt.

11 Übermittlungen durch Benutzer

Sie können Spam, Phishing und andere in ihrem Posteingang eingetroffene unerwünschte Nachrichten bzw. solche, die fälschlicherweise isoliert wurden, identifizieren und an den McAfee Quarantine Manager übermitteln, um sie freigeben zu lassen.

Isolierte Elemente müssen immer an den McAfee Quarantine Manager-Administrator übermittelt werden, wenn Sie der Meinung sind, dass sie freigegeben oder zur Analyse an McAfee Labs übermittelt werden sollten.

Der McAfee Quarantine Manager-Administrator überprüft die durch Benutzer übermittelten Nachrichten und führt für diese die entsprechenden Aktionen durch, je nachdem, ob sie:

- von Benutzern übermittelt wurden, da sie fälschlicherweise als Spam eingestuft wurden,
- als Spam übermittelt wurden,
- zur Freigabe übermittelt wurden (die Nachricht also kein Spam oder anderweitig unerwünschtes Objekt ist).

Inhalt

- *Verwalten der Übermittlungen durch Benutzer*
- *Anzeigen von Suchergebnissen*

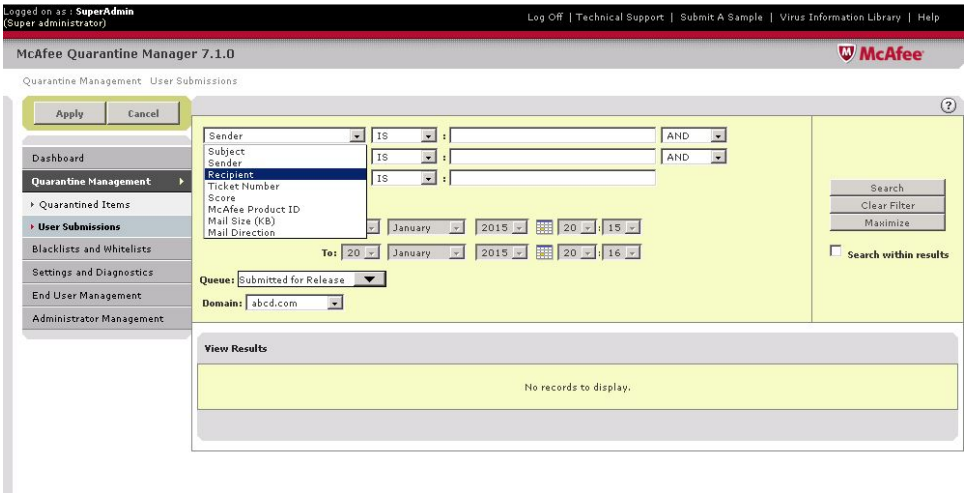
Verwalten der Übermittlungen durch Benutzer

Zum Suchen und Anzeigen von Übermittlungen durch Benutzer müssen Sie verschiedene Filterebenen zuordnen.

Vorgehensweise

1. Klicken Sie im Menü von McAfee Quarantine Manager auf **Quarantäne-Management** | **Übermittlungen durch Benutzer** (Systemlisten | SSO-Katalog).
2. Wählen Sie in der Dropdown-Liste **Warteschlange** den Übermittlungstyp aus.

3 Wählen Sie bis zu drei Filter der obersten Ebene aus.



4 Wenn Sie nach einer bestimmten Domäne suchen möchten, wählen Sie diese in der Dropdown-Liste **Domäne** aus.

5 Legen Sie den Zeitraum fest.

6 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird nun eine Liste der Elemente angezeigt, die Ihren Suchkriterien entsprechen.

Anzeigen von Suchergebnissen

Sie können für ausgewählte isolierte Elemente bestimmte Aktionen durchführen.

Vorgehensweise

- Unter **Ergebnisse anzeigen** können Sie für zuvor ausgewählte isolierte Elemente bestimmte Aktionen durchführen.

12 Benutzerinteraktionen

Über die McAfee Quarantine Manager-Benutzeroberfläche können Sie Ihre isolierten E-Mail-Nachrichten verwalten, Spam-Proben an McAfee übermitteln und Ihr McAfee Quarantine Manager-Konto verwalten.

Als Benutzer können Sie über die McAfee Quarantine Manager-Benutzeroberfläche Folgendes durchführen:

- Verwalten Ihres McAfee Quarantine Manager-Kontos.
- Anzeigen und Verwalten Ihrer isolierten Elemente.
- Anzeigen und Verwalten einer persönlichen Blacklist und Whitelist.
- Freigeben von Nachrichten, die fälschlicherweise isoliert wurden.
- Einsenden nicht entdeckter Spam-Nachrichten an McAfee Labs, damit ähnliche Nachrichten zukünftig entdeckt und isoliert werden können.

Inhalt

- *Anmelden bei McAfee Quarantine Manager*
- *Verwalten von isolierten E-Mails über die Benutzeroberfläche*
- *Verwalten von isolierten E-Mails über Digest-E-Mails*
- *Übermitteln von Spam-Proben an McAfee Labs*
- *Verwalten Ihres McAfee Quarantine Manager-Kontos*

Anmelden bei McAfee Quarantine Manager

Melden Sie sich bei McAfee Quarantine Manager an, um Ihr Konto zu verwalten oder zu ändern.

Vorgehensweise

1. Rufen Sie zum Öffnen der Benutzeroberfläche in einem Web-Browser die Adresse http://<MQMServer>/MQMUserUI/<lokaleID>/LogOn.html auf.
2. Melden Sie sich als Benutzer an.
   - **LDAP-Authentifizierung**: Wenn Ihr Unternehmen einen LDAP-Server verwendet und Ihr Administrator die LDAP-Authentifizierung aktiviert hat, können Sie sich mit dem Benutzernamen und Kennwort des LDAP-Kontos bei McAfee Quarantine Manager anmelden.
   - **Quarantine Manager-Authentifizierung**: Wenn Ihr Administrator die Authentifizierung über das **Quarantine Manager-Konto** aktiviert hat, können Sie sich bei McAfee Quarantine Manager mit dem Benutzernamen und dem Kennwort Ihres McAfee Quarantine Manager-Kontos anmelden.

3 Wenn Sie McAfee Quarantine Manager zum ersten Mal verwenden und Ihr Unternehmen die McAfee Quarantine Manager-Authentifizierung verwendet, richten Sie Ihre McAfee Quarantine Manager-Anmeldung wie folgt ein:

   a Klicken Sie auf **Neuer Benutzer? Zum Registrieren hier klicken**.

   b Geben Sie im Dialogfeld **Benutzerregistrierung** Ihre **E-Mail-Adresse** ein, und klicken Sie dann auf **Registrieren**.

   Nun wird Ihnen in einer Meldung bestätigt, dass ein Konto erstellt und ein Standardkennwort an Ihre E-Mail-Adresse gesendet wurde. Klicken Sie zum Bestätigen auf **OK**.

   c Klicken Sie abschließend auf **Klicken Sie hier, um zur Anmeldeseite zurückzukehren**, und melden Sie sich mit den Anmeldeinformationen, die Sie in der E-Mail erhalten haben, bei McAfee Quarantine Manager an.

Standardmäßig wird die Seite **Isolierte Objekte** angezeigt. Auf dieser Seite sind die an Sie gerichteten E-Mails aufgeführt, die entdeckt und isoliert wurden. Sie können für die Suche nach isolierten Elementen, die für Sie von Interesse sind, Suchfilter verwenden. Darüber hinaus können Sie auf dieser Seite die isolierten E-Mails analysieren und freigeben, sie der Blacklist oder Whitelist hinzufügen oder sie zur Analyse an McAfee übermitteln.

Verwalten von isolierten E-Mails über die Benutzeroberfläche

Sie können eine Liste von erhaltenen E-Mails anzeigen, die erkannt und isoliert wurden, damit Sie sie analysieren und entsprechende Maßnahmen ergreifen können.

Sie können die folgenden Verwaltungsschritte durchführen:

- Freigeben von Elemente, die fälschlicherweise isoliert wurden, an Ihr Postfach,
- Löschen von Spam-Nachrichten und Eintragen ihrer Absender in die Blacklist,
- Löschen der ausgewählten oder aller Elemente ohne weitere Aktion,
- Eintragen von vertrauenswürdigen Absendern in Ihre Whitelist,
- Suchen nach bestimmten isolierten Elementen anhand von Suchfiltern.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Rufen Sie in **Ergebnisse anzeigen** die Liste der isolierten E-Mails auf.

Standardmäßig werden auf jeder Seite 20 Elemente angezeigt. Sie können die Zahl der Datensätze pro Seite angeben, indem Sie in der Dropdown-Liste **10**, **20**, **50** oder **100** auswählen. Sie können mit den Schaltflächen **Weiter**, **Zurück**, **Erste** und **Letzte** durch die Seiten navigieren.

3 Wenn Sie Spalten ergänzen oder entfernen möchten, klicken Sie auf **Anzuzeigende Spalten**, und wählen Sie die gewünschten Spalten aus.

4 Wählen Sie eine oder mehrere E-Mails aus, und führen Sie dann die gewünschte Aktion durch.

Wenn die Warteschlangen nicht ausgewählt sind oder der Ergebnisdatensatz kein Element aus diesen Warteschlangen enthält, werden einige Aktionen möglicherweise nicht angezeigt. Wenn Sie beispielsweise in den Suchfiltern unter **Warteschlange** nicht **Spam** ausgewählt haben, werden Aktionen wie **Übermitteln als Nicht-Spam**, **In Whitelist aufnehmen und freigeben** und **Übermitteln als Nicht-Spam und in Whitelist aufnehmen** usw. nicht angezeigt. Mit dem Kontrollkästchen in der Kopfzeile können Sie alle Elemente im Raster auf einmal auswählen bzw. die Auswahl aller Elemente aufheben.

5 Erstellen Sie Suchfilter, um nach isolierten Elementen zu suchen.

a Wählen Sie für jeden Filter ein Vergleichskriterium aus.

- **IST**: Stimmt mit einem Wert überein, der dem angegebenen Wert entspricht.
- **IST NICHT**: Stimmt mit einem Wert überein, der dem angegebenen Wert NICHT entspricht.

b Sie können auch diese Platzhalter verwenden:

- `*`: Entspricht einer beliebigen Anzahl von Zeichen.
- `?`: Entspricht einem einzelnen Zeichen.
- `\\`: Entspricht einem umgekehrten Schrägstrich (`\`) im Suchfeld.

c Wählen Sie den Operator für die Verwendung mehrerer Suchfilter aus.

- **UND**: Es werden die früheren und die letzten Filter werden berücksichtigt.
- **ODER**: Es werden entweder die früheren oder die letzten Filter berücksichtigt.

d Wiederholen Sie die Schritte, wenn Sie weitere Filter verwenden möchten.

6 Wählen Sie in den Dropdown-Listen die Option **Alle Daten** oder einen gewünschten **Datumsbereich** aus.

7 Wählen Sie eine Warteschlange aus, um nach isolierten Elementen anhand ihrer Klassifizierung zu suchen.

8 Klicken Sie auf **Suchen**, um die auf den oben ausgewählten Kriterien basierende Suche zu starten. Klicken Sie auf **Filter löschen**, um zu den Standardfiltereinstellungen zurückzukehren.

Sie können anhand des **UND**- bzw. **ODER**-Operators bis zu drei Filter verwenden. So rufen Sie beispielsweise eine Liste der isolierten Elemente ab, deren Betreff das Wort *Angebot* enthält und die von *xyz@abc.com* gesendet wurden:

a Wählen Sie **Betreff** aus.

b Wählen Sie **Ist** aus, und geben Sie dann `Angebot` ein.

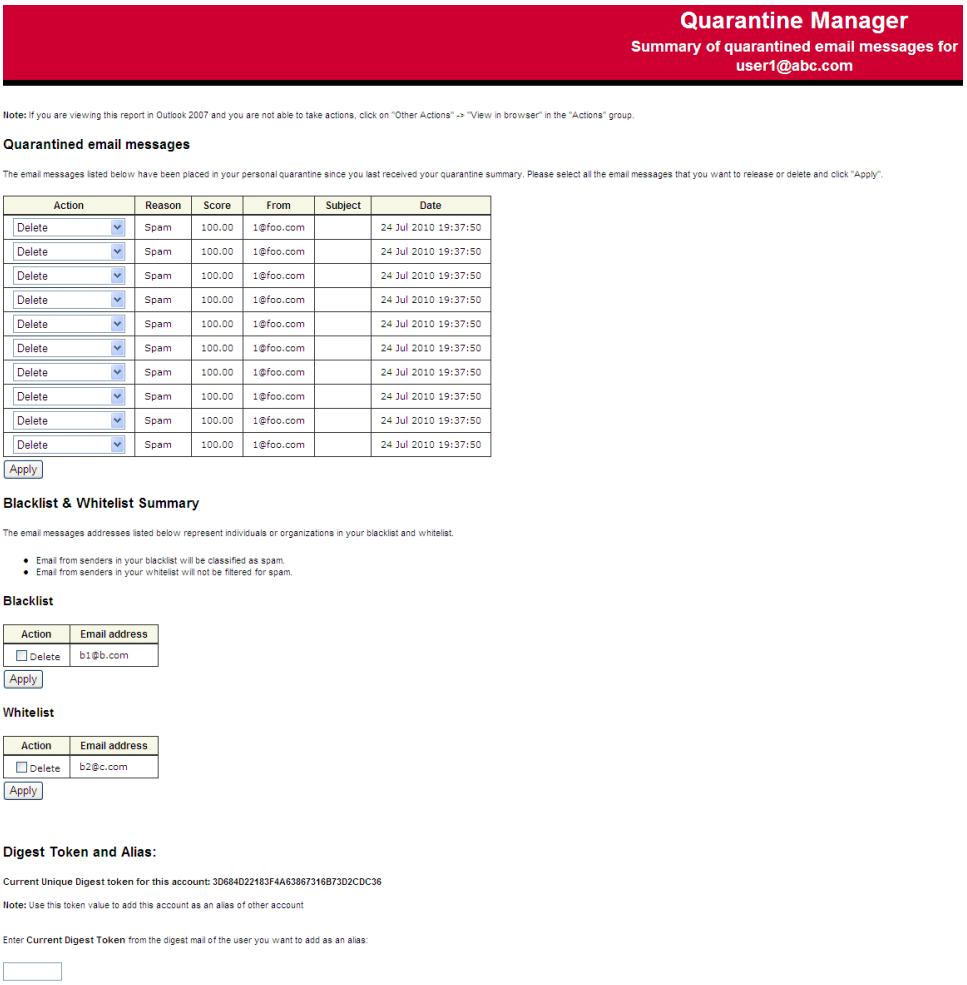
c Wählen Sie **Und** | **Absender** aus.

d Wählen Sie **Ist** aus, und geben Sie dann „xyz@abc.com" ein.

Verwalten von isolierten E-Mails über Digest-E-Mails

Sie können Ihre isolierten E-Mails mithilfe von Digest-E-Mail-Aktionen verwalten.

Eine Digest-E-Mail enthält eine anpassbare Zusammenfassung Ihrer isolierten Elemente und Black-/Whitelists sowie der zugehörigen Quarantäne-Aktivitäten. Die in der Digest-E-Mail enthaltenen Informationen hängen von den Administratorkonfigurationen ab.



Quarantine Manager
Summary of quarantined email messages for user1@abc.com

Note: If you are viewing this report in Outlook 2007 and you are not able to take actions, click on "Other Actions" -> "View in browser" in the "Actions" group.

Quarantined email messages

The email messages listed below have been placed in your personal quarantine since you last received your quarantine summary. Please select all the email messages that you want to release or delete and click "Apply".

Action	Reason	Score	From	Subject	Date
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50
Delete	Spam	100.00	1@foo.com		24 Jul 2010 19:37:50

Apply

Blacklist & Whitelist Summary

The email messages addresses listed below represent individuals or organizations in your blacklist and whitelist.

- Email from senders in your blacklist will be classified as spam.
- Email from senders in your whitelist will not be filtered for spam.

Blacklist

Action	Email address
Delete	b1@b.com

Apply

Whitelist

Action	Email address
Delete	b2@c.com

Apply

Digest Token and Alias:

Current Unique Digest token for this account: 3D684D22183F4A63867316B73D2CDC36

Note: Use this token value to add this account as an alias of other account

Enter **Current Digest Token** from the digest mail of the user you want to add as an alias:

Vorgehensweise

1 Öffnen Sie die Digest-E-Mail.

2 Führen Sie die Digest-E-Mail-Aktionen aus.

Falls Ihr Administrator dies konfiguriert hat, wird für jede Aktion eine Antwortnachricht angezeigt.

Übermitteln von Spam-Proben an McAfee Labs

Sie können E-Mail-Nachrichten als Spam-Proben an McAfee Labs senden. Speichern Sie die E-Mail hierfür zunächst als EML-Datei. Sie können Spam-Proben übermitteln, wenn Spam-E-Mails fälschlicherweise für in Ihr Postfach freigegeben wurden und Sie diese zur Analyse übermitteln möchten.

E-Mails werden vor dem Senden an McAfee Labs von Administratoren überprüft.

Bei McAfee Labs werden die E-Mail-Nachrichten dann auf ihre Eigenschaften hin analysiert. Je mehr E-Mails zur Korrektur übermittelt werden, desto präziser wird die Nachrichtenfilterung.

So übermitteln Sie Spam-Proben:

- Senden Sie einen Datenträger mit den Spam-Proben an Ihren Administrator.
- Verwenden Sie hierfür die Menüleistenoption **Spam- oder Phishing-Probe übermitteln** in Ihrem E-Mail-Client.
- Verwenden Sie die Seite **Spam-Probe übermitteln** auf der McAfee Quarantine Manager-Benutzeroberfläche.

Aufgaben

- *Übermitteln von auf einem Datenträger gespeicherten Spam-Proben* auf Seite 71
  Sie können Spam-Proben übermitteln, die als EML-Dateien auf Ihrem Computer gespeichert sind.
- *Übermitteln von Spam-Proben mit dem Customer Submission Tool von McAfee* auf Seite 71
  Mithilfe des McAfee Customer Submission Tool können Sie Spam-Proben auch direkt aus Microsoft Outlook übermitteln.
- *Übermitteln einer Probe eines fälschlicherweise isolierten Elements* auf Seite 72
  Sie können Proben von isolierten E-Mails übermitteln, die fälschlicherweise als Spam klassifiziert wurden, bei denen Sie jedoch sicher sind, dass sie aus vertrauenswürdigen Quellen stammen.

Übermitteln von auf einem Datenträger gespeicherten Spam-Proben

Sie können Spam-Proben übermitteln, die als EML-Dateien auf Ihrem Computer gespeichert sind.

Vorgehensweise

1. Speichern Sie die als Spam zu übermittelnden E-Mails in Ihrem E-Mail-Client als EML-Dateien.
2. Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.
3. Klicken Sie auf **Spam-Probe übermitteln** | **Durchsuchen**, und navigieren Sie dann zu den EML-Dateien.
4. Klicken Sie auf **Übermitteln**, um die Spam-Proben an Ihren Administrator zu senden.

   Der Administrator überprüft diese E-Mail-Nachrichten und übermittelt sie anschließend an McAfee Labs. Bei McAfee Labs werden die E-Mail-Nachrichten dann auf ihre Eigenschaften hin analysiert.

Übermitteln von Spam-Proben mit dem Customer Submission Tool von McAfee

Mithilfe des McAfee Customer Submission Tool können Sie Spam-Proben auch direkt aus Microsoft Outlook übermitteln.

> **Bevor Sie beginnen**
>
> Das McAfee Customer Submission Tool muss vom Administrator installiert werden.

Vorgehensweise

1 Wählen Sie in Microsoft Outlook die zu übermittelnden E-Mails aus.

2 Klicken Sie in der Menüleiste auf eine der folgenden Spam-Optionen:

- **Spam-Probe übermitteln**
- **Nicht-Spam-Probe übermitteln**

3 Wählen Sie im Fenster **Spam- oder Phishing-Probe übermitteln** die gewünschten Aktionen aus, und klicken Sie dann auf **OK**.

Der Administrator überprüft die von Ihnen übermittelten E-Mail-Nachrichten und übermittelt sie anschließend an McAfee Labs. Bei McAfee Labs werden die E-Mail-Nachrichten dann auf ihre Eigenschaften hin analysiert.

Übermitteln einer Probe eines fälschlicherweise isolierten Elements

Sie können Proben von isolierten E-Mails übermitteln, die fälschlicherweise als Spam klassifiziert wurden, bei denen Sie jedoch sicher sind, dass sie aus vertrauenswürdigen Quellen stammen.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Wählen Sie die isolierte E-Mail aus, die fälschlicherweise als Spam klassifiziert wurde.

3 Wählen Sie **Weitere Aktionen** | **Übermitteln als Nicht-Spam** aus, und klicken Sie dann auf **Los**.

Der Administrator überprüft diese E-Mail-Nachricht und übermittelt sie anschließend an McAfee Labs. Bei McAfee Labs wird die E-Mail-Nachricht dann auf ihre Eigenschaften hin analysiert.

Verwalten Ihres McAfee Quarantine Manager-Kontos

Sie können die verschiedenen Einstellungen in Ihrem McAfee Quarantine Manager-Konto verwalten.

Sie können die folgenden Verwaltungsschritte für Ihr McAfee Quarantine Manager-Konto durchführen:

- Verwalten Ihrer Blacklist und Whitelist durch Hinzufügen bzw. Entfernen von E-Mail-Adressen.
- Hinzufügen alternativer E-Mail-Adressen, damit sich die isolierten Elemente an einer gemeinsamen Stelle befinden.
- Ändern Ihres Kennworts.
- Angeben der Speicherdauer (in Tagen) isolierter Elemente. Dieses Limit kann von dem Limit überschrieben werden, das der Administrator festlegt.
- Anzeigen der Liste der isolierten Elemente von Benutzern, die Sie verwalten.

Aufgaben

- *Verwalten der Blacklist* auf Seite 73
  Sie können Ihre Blacklist verwalten, die die E-Mail-Adressen enthält, von denen Sie häufig Spam-Mails oder unerwünschte E-Mails erhalten.
- *Verwalten der Whitelist* auf Seite 73
  Die Whitelist enthält als vertrauenswürdig eingestufte Absender-E-Mail-Adressen. Diese Liste können Sie verwalten, indem Sie beispielsweise Geschäftspartner hinzufügen, deren E-Mails Sie empfangen möchten.
- *Ändern des Kennworts* auf Seite 74
  Sie können Ihr Kontokennwort ändern.
- *Konfigurieren der Voreinstellungen für den Quarantäne-Bericht* auf Seite 74
  Sie können die Voreinstellungen für die Zusendung von Berichten über die Isolierungsaktivitäten konfigurieren.
- *Verwalten von Aliassen* auf Seite 75
  Sie können Ihre E-Mail-Aliasse verwalten. E-Mail-Aliasse können verwendet werden, wenn Sie über mehrere E-Mail-Adressen verfügen.
- *Anzeigen von E-Mail-Neuzuweisungen* auf Seite 75
  Sie können eine Liste der Benutzer und der isolierten Elemente anzeigen, die Sie verwalten.

Verwalten der Blacklist

Sie können Ihre Blacklist verwalten, die die E-Mail-Adressen enthält, von denen Sie häufig Spam-Mails oder unerwünschte E-Mails erhalten.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Wählen Sie **Ihr Konto** | **Blacklist** aus.

3 Geben Sie E-Mail-Adressen, die der Liste hinzugefügt werden sollen, im Feld **E-Mail-Adresse** ein, und klicken Sie dann auf **Hinzufügen**.

Die E-Mail-Adresse wird in der Liste **Mitglieder** angezeigt.

4 Klicken Sie zum Löschen einer einzelnen E-Mail-Adresse aus der Blacklist auf ✖. Klicken Sie zum Löschen von allen E-Mail-Adressen in der Blacklist auf **Alle Löschen**.

Daraufhin wird eine Bestätigungsmeldung angezeigt.

5 Klicken Sie zum Abschluss des Löschvorgangs im angezeigten Dialogfeld auf **OK**. Klicken Sie zum Verwerfen der Änderungen auf **Abbrechen**.

6 Klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

Verwalten der Whitelist

Die Whitelist enthält als vertrauenswürdig eingestufte Absender-E-Mail-Adressen. Diese Liste können Sie verwalten, indem Sie beispielsweise Geschäftspartner hinzufügen, deren E-Mails Sie empfangen möchten.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Wählen Sie **Ihr Konto** | **Whitelist** aus.

3 Geben Sie E-Mail-Adressen, die der Liste hinzugefügt werden sollen, im Feld **E-Mail-Adresse** ein, und klicken Sie dann auf **Hinzufügen**.

Die E-Mail-Adresse wird nun in der Liste **Mitglieder** angezeigt.

4 Klicken Sie zum Löschen einzelner E-Mail-Adressen aus der Whitelist auf ✖. Wenn Sie alle in der Whitelist enthaltenen Adressen löschen möchten, klicken Sie auf **Alle löschen**.

Daraufhin wird eine Bestätigungsmeldung angezeigt.

5 Klicken Sie zum Abschluss des Löschvorgangs im angezeigten Dialogfeld auf **OK**. Klicken Sie zum Verwerfen der Änderungen auf **Abbrechen**.

6 Klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

Ändern des Kennworts

Sie können Ihr Kontokennwort ändern.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Wählen Sie **Ihr Konto** | **Einstellungen** aus.

3 Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.

Das neue Kennwort darf nur Buchstaben und Ziffern enthalten und muss aus mindestens acht Zeichen bestehen. Wenn der Authentifizierungsmodus auf **LDAP-Benutzerkonten** eingestellt ist, können Sie das Kennwort nicht ändern.

4 Geben Sie im Feld **Neues Kennwort bestätigen** das neue Kennwort ein.

5 Klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

Konfigurieren der Voreinstellungen für den Quarantäne-Bericht

Sie können die Voreinstellungen für die Zusendung von Berichten über die Isolierungsaktivitäten konfigurieren.

Vorgehensweise

1 Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.

2 Wählen Sie **Ihr Konto** | **Einstellungen** aus.

3 Geben Sie unter **Konfigurationseinstellungen** Ihre Voreinstellungen für Digest-E-Mails an.

- Wenn Sie E-Mail-Digests über Ihre isolierten Elemente und die Black- und Whitelists erhalten möchten, wählen Sie **Ich möchte Digest-Berichte zur Isolierungsaktivität erhalten** aus.
- Wenn Sie zu jedem geplanten Digest E-Mail-Digests erhalten möchten, auch wenn für Ihr Konto keine isolierten Elemente vorhanden sind, wählen Sie **Digest senden, auch wenn keine isolierten Objekte vorhanden sind** aus.

4 Klicken Sie zum Speichern der Änderungen auf **Übernehmen**.

Verwalten von Aliassen

Sie können Ihre E-Mail-Aliasse verwalten. E-Mail-Aliasse können verwendet werden, wenn Sie über mehrere E-Mail-Adressen verfügen.

Angenommen, das Unternehmen, für das Sie arbeiten, ändert Ihre E-Mail-Adresse, Sie möchten Ihre alte E-Mail-Adresse jedoch weiterhin verwenden können. Wenn Sie die alte Adresse als Alias hinzufügen, können isolierte E-Mails, die für eine der beiden Adressen bestimmt sind, am gleichen Ort gefunden werden. Wenn Sie einen Alias hinzufügen, wird der Aktivierungscode an die Alias-Adresse gesendet. Die Änderungen werden als anstehende Aktivierung angezeigt und werden erst gültig, wenn Sie den Aktivierungscode angeben.

Wenn Ihr Administrator die LDAP-Authentifizierung aktiviert hat, können Sie alle E-Mail-Aliasse einsehen, die für Sie auf dem LDAP-Server vorhanden sind. Sie können jedoch keine Änderungen daran vornehmen oder neue Aliasse hinzufügen.

Vorgehensweise

1. Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.
2. Wählen Sie **Ihr Konto** | **E-Mail-Aliasse** aus.
3. Geben Sie im Feld **Name** den E-Mail-Alias ein, und klicken Sie anschließend auf **Hinzufügen**.

   Der Alias wird in der Liste angezeigt, und Sie werden zur Eingabe eines Aktivierungscodes aufgefordert.
4. Klicken Sie auf **Übernehmen**, damit der Aktivierungscode an Ihre E-Mail-Adresse gesendet wird.
5. Geben Sie im Feld **Aktivierungscode hier eingeben** den Aktivierungscode ein, und klicken Sie dann auf **Aktivieren**.
6. Klicken Sie auf **OK**.
7. Klicken Sie zum Löschen eines E-Mail-Alias in der Spalte **Löschen** neben dem zu löschenden Alias auf ✖.
8. Klicken Sie zum Speichern der Änderungen auf **OK** | **Übernehmen** (Systemlisten | SSO-Katalog).

Anzeigen von E-Mail-Neuzuweisungen

Sie können eine Liste der Benutzer und der isolierten Elemente anzeigen, die Sie verwalten.

Vorgehensweise

1. Melden Sie sich bei der Benutzeroberfläche von McAfee Quarantine Manager an.
2. Wählen Sie **Ihr Konto** | **E-Mail-Neuzuweisung** aus.

Pflege und Berichterstellung

Halten Sie Ihre Blacklists und Whitelists auf dem aktuellen Stand, und verwalten Sie die wichtigsten Funktionen von McAfee Quarantine Manager über das Dashboard und die Berichterstellungsfunktion.

Kapitel 13 *Server-Wartung*

Kapitel 14 *Verwaltung von Blacklists und Whitelists*

Kapitel 15 *Dashboard und grafische Berichte*

13 Server-Wartung

Sie können Server-Konfigurationen verwalten, Datenbanksicherungen erstellen, mehrere isolierte Elemente auf einmal freigeben und Neuzuweisungslisten für verbundene McAfee-Produkte erstellen.

Inhalt

- *Verwalten der Server-Konfigurationen*
- *Sichern der Datenbank*

Verwalten der Server-Konfigurationen

Legen Sie die Parameter für **Produktprotokoll**, **Diagnose**, **Kommunikation** und **Erweiterte Einstellungen** fest.

Aufgaben

- *Anzeigen von Protokolleinträgen* auf Seite 79
  Sie können den Zustand des McAfee Quarantine Manager-Servers anhand der Protokolleinträge zu Ereignissen, Warnungen und Fehlern überprüfen.
- *Konfigurieren der Protokolleinstellungen* auf Seite 80
  Sie können die gewünschte Art der Protokollierung sowie die Debug-Verfolgungsstufe angeben und die Einstellungen für Fehlerberichte konfigurieren.
- *Konfigurieren der Kommunikation zwischen MQM und anderen Produkten* auf Seite 81
  Sie können die MQM-Einstellungen für die Kommunikation mit McAfee-Produkten, LDAP-Servern und E-Mail-Servern konfigurieren.
- *Konfigurieren der erweiterten Server-Einstellungen* auf Seite 82
  Sie können die erweiterten McAfee Quarantine Manager-Einstellungen konfigurieren. Dies umfasst die Voreinstellungen für ePolicy Orchestrator-Ereignisse, Übermittlungen an McAfee Labs, das Sitzungszeitlimit und die Dashboard-Aktualisierungsintervalle.
- *Konfigurieren von Zertifikaten für die sichere SMTP-Kommunikation* auf Seite 86
  Sie können Zertifikate für die sichere (TLS) SMTP-Kommunikation konfigurieren.

Anzeigen von Protokolleinträgen

Sie können den Zustand des McAfee Quarantine Manager-Servers anhand der Protokolleinträge zu Ereignissen, Warnungen und Fehlern überprüfen.

Sie können die gewünschten Protokolleinträge mithilfe der Suchfilter finden. Suchen Sie Informationen über gestartete bzw. beendete Tasks, verbundene bzw. getrennte Produkte oder Fehler im Zusammenhang mit fehlgeschlagenen Übertragungen von Konfigurationseinstellungen an ein Produkt.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Einstellungen und Diagnose** | **Produktprotokoll** (Systemlisten | SSO-Katalog).

2 Konfigurieren Sie die Suchfilter.

   a Wählen Sie für jeden Filter ein Vergleichskriterium aus.

   b Wählen Sie einen geeigneten logischen Operator aus, wenn Sie mehrere Suchfilter verwenden möchten.

3 Wählen Sie das Datum aus, für das Sie das Protokoll einsehen möchten.

4 Klicken Sie auf **Suchen**.

5 Im Abschnitt **Ergebnisse anzeigen** werden nun die Produktprotokolleinträge für Ereignisse, Warnungen und Fehler angezeigt.

Konfigurieren der Protokolleinstellungen

Sie können die gewünschte Art der Protokollierung sowie die Debug-Verfolgungsstufe angeben und die Einstellungen für Fehlerberichte konfigurieren.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Einstellungen und Diagnose** | **Diagnose** | **Protokollierung**, und konfigurieren Sie dann die verfügbaren Optionen.

2 Konfigurieren Sie die Optionen auf der Seite **Debug-Verfolgung**.

   a Wählen Sie in der Dropdown-Liste **Stufe** eine Stufe für die Protokollierung der Fehlerbehebung aus.

   b Wählen Sie in der Dropdown-Liste **Speicherort** den Speicherort für die Debug-Verfolgungsdateien aus.

   c Klicken Sie auf **Herunterladen**, um die Debug-Verfolgungsdateien auf die Festplatte zu exportieren.

   d Geben Sie im Feld **Maximale Dateigröße (MB)** die maximale Größe der Debug-Verfolgungsdateien ein.

   e Wählen Sie zur Angabe einer unbegrenzten Größe **Unbegrenzt** aus.

3 Wählen Sie unter **Protokollierung** aus, ob Informationen, Warnungen und Fehlerereignisse über das Produktprotokoll oder das Windows-Ereignisprotokoll protokolliert werden sollen.

   Standardmäßig werden Ereignisse im Produktprotokoll protokolliert.

4 Konfigurieren Sie die Optionen auf der Seite **Fehlerberichterstellung**.

   a Zum Aktivieren oder Deaktivieren des Fehlerberichterstellungsdienstes wählen Sie **Aktivieren** aus.

   b Mithilfe von **Ausnahmen erfassen** können Sie die Erfassung von Daten zu außergewöhnlichen Ereignissen (schwerwiegende Ausnahmefehler) wie beispielsweise Systemabstürze aktivieren bzw. deaktivieren.

   c Zum Aktivieren oder Deaktivieren von nicht behandelten Ausnahmen für Administratorberichte wählen Sie **Ausnahmen auf dem Bildschirm melden** aus.

Konfigurieren der Kommunikation zwischen MQM und anderen Produkten

Sie können die MQM-Einstellungen für die Kommunikation mit McAfee-Produkten, LDAP-Servern und E-Mail-Servern konfigurieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Melden Sie sich als Administrator bei McAfee ePO an.

2 Klicken Sie im Hauptmenü von MQM auf **Einstellungen und Diagnose** | **Kommunikation** | **Standard**, und konfigurieren Sie dann die Optionen.

3 Wählen Sie unter **McAfee-Produkte** die Port-Nummer aus, die Sie für die Verbindung verwenden möchten.

4 Klicken Sie auf **Mail-Server**, und geben Sie die Details der SMTP-Server-Kommunikation mit den Benutzern an.

- **Adresse**: die IP-Adresse oder der DNS-Host-Name des E-Mail-Servers.
- **Port-Nummer**: die Nummer des Ports, der für die ausgehende E-Mail-Kommunikation verwendet werden soll. Standardmäßig wird hierfür Port 25 verwendet.
- **TLS**: Wählen Sie diese Option aus, um TLS (Transport Layer Security) zur Absicherung der gesamten E-Mail-Kommunikation zu verwenden.

Wenn Sie TLS auswählen, muss sich das E-Mail-Server-Zertifikat im MQM-Installationsordner befinden.

5 Klicken Sie auf **LDAP-Server**, und konfigurieren Sie die Optionen.

Es können mehrere LDAP-Server konfiguriert werden.

a Wählen Sie in der Dropdown-Liste **Server-Typ** den LDAP-Server aus.

b Geben Sie im Feld **Server** die IP-Adresse oder den Domänennamen des LDAP-Servers ein.

c Geben Sie im Feld **Port** die Port-Nummer ein, die für die Kommunikation mit dem LDAP-Server verwendet wird.

d Wählen Sie für eine sichere Verbindung die Option **SSL verwenden** aus.

e Geben Sie im Feld **Benutzername** den Benutzernamen für den LDAP-Server ein.

f Geben Sie im Feld **Kennwort** das Benutzerkennwort ein.

g Geben Sie im Feld **Basis-DN** den Namen der Organisationseinheit im LDAP-Server ein.

h Geben Sie im Feld **Objektklasse für Verteilerlisten** die Objektklassen-ID für Verteilerlisten für den Open LDAP-Server ein.

i Geben Sie im Feld **Name des Mitgliedsattributs in der Objektklasse für Verteilerlisten** das Mitgliedsattribut der Objektklasse für Verteilerlisten ein.

j Klicken Sie auf **Testen**, um die Verbindung mit dem LDAP-Server zu überprüfen.

k Klicken Sie zum Speichern der Einstellungen auf **Übernehmen**.

l Klicken Sie auf **Abbrechen**, um die Änderungen rückgängig zu machen und zu den Standardeinstellungen zurückzukehren.

6 Klicken Sie auf **Erweitert**, und konfigurieren Sie die Optionen.

a Geben Sie im Feld **Größe des Thread-Pools** ein, wie viele Threads gleichzeitig für die Verarbeitung eingehender isolierter Elemente ausgeführt werden können, und starten Sie MQM dann neu.

b Geben Sie im Feld **Maximale Kommunikationswiederholungen** ein, wie häufig der MQM-Server zur Übertragung von Konfigurationen oder Freigabe von isolierten E-Mails im Höchstfall versuchen soll, eine Kommunikationsverbindung mit einem verbundenen McAfee-Produkt herzustellen.

c Geben Sie im Feld **Konfigurationsübertragungsintervall (in Sekunden)** den Abstand zwischen Blacklist-, Whitelist- und Benutzergruppenaktualisierungen auf verbundenen McAfee-Produkten ein.

d Geben Sie im Feld **Objektübertragungsintervall (in Sekunden)** den Abstand zwischen den Aktualisierungen von isolierten Elementen zur Freigabe auf verbundenen McAfee-Produkten ein.

Siehe auch

Konfigurieren von Zertifikaten für die sichere SMTP-Kommunikation auf Seite 86

Konfigurieren der erweiterten Server-Einstellungen

Sie können die erweiterten McAfee Quarantine Manager-Einstellungen konfigurieren. Dies umfasst die Voreinstellungen für ePolicy Orchestrator-Ereignisse, Übermittlungen an McAfee Labs, das Sitzungszeitlimit und die Dashboard-Aktualisierungsintervalle.

Aufgaben

- *Konfigurieren der Einstellungen für McAfee ePO* auf Seite 82
  Sie können das Erstellen von McAfee ePO-Ereignissen und die Häufigkeit, mit der Ereignisse im MQM generiert werden, für die Berichterstellung in McAfee ePO konfigurieren.
- *Konfigurieren der Datenbankeinstellungen* auf Seite 83
  Durch das Konfigurieren der Datenbankeinstellungen kann die optimale Leistungsfähigkeit der Datenbank erreicht werden.
- *Konfigurieren der Server-Kommunikation mit McAfee Labs* auf Seite 83
  Sie müssen SMTP-Server-Details angeben, damit MQM Daten und Elemente an McAfee Labs übermitteln kann. Dies ist der SMTP-Server, der E-Mails aus Ihrem Netzwerk sendet.
- *Konfigurieren der Einstellungen für E-Mail-Benachrichtigungen* auf Seite 84
  Sie können Absender- und Empfänger-E-Mail-Adressen für Benachrichtigungs-E-Mails von MQM angeben.
- *Konfigurieren verschiedener Einstellungen* auf Seite 84
  Konfigurieren Sie die Parameter für verschiedene Einstellungen.
- *Konfigurieren der Einstellungen für Statusbericht-E-Mails* auf Seite 85
  Sie können die Status-E-Mail vor dem Senden an Administratoren in der Vorschau anzeigen, bearbeiten und anpassen.
- *Gleichzeitiges Freigeben mehrerer E-Mails* auf Seite 85
  Sie können Parameter für die Massenfreigabe von E-Mails festlegen. Es können mehr als 100 E-Mails auf einmal freigegeben werden.
- *Neuzuweisen von aus der Quarantäne freigegebenen E-Mails zu anderen Produkten* auf Seite 86
  Sie können isolierte E-Mails eines McAfee-Produkts durch ein anderes Produkt freigeben. MQM gibt eine E-Mail über das McAfee-Produkt frei, das die E-Mail isoliert hat.

Konfigurieren der Einstellungen für McAfee ePO

Sie können das Erstellen von McAfee ePO-Ereignissen und die Häufigkeit, mit der Ereignisse im MQM generiert werden, für die Berichterstellung in McAfee ePO konfigurieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in MQM **Einstellungen und Diagnose** | **Erweiterte Einstellungen** aus.
2. Wählen Sie zum Generieren von McAfee ePO-Ereignissen **ePolicy Orchestrator-Ereignisse generieren** aus.
3. Geben Sie im Feld **Erzeugungsintervall für ePolicy Orchestrator-Ereignisse (in Minuten)** das Intervall ein.

   Der Standardwert ist 10.
4. Starten Sie den McAfee Quarantine Manager-Dienst neu.

Sie können Ereignisberichte in McAfee ePO anzeigen.

Konfigurieren der Datenbankeinstellungen

Durch das Konfigurieren der Datenbankeinstellungen kann die optimale Leistungsfähigkeit der Datenbank erreicht werden.

Vorgehensweise

1. Wählen Sie in MQM **Einstellungen und Diagnose** | **Datenbankverwaltung** aus.
2. Geben Sie im Feld **Maximale Elementgröße (MB)** die höchstzulässige Größe eines isolierten Elements für die Datenbank an.

   Wenn die Größe eines isolierten Elements die angegebene Größe überschreitet, wird das Element an das McAfee-Produkt zurückgegeben. MQM unterstützt hier eine maximale Größe von 100 MB.
3. Geben Sie unter **Maximale Abfragegröße** an, wie viele Zeilen bei einer Abfrage maximal zurückgegeben werden sollen.

   Wenn Sie mehr als die festgelegte Anzahl an Elementen anzeigen möchten, können Sie durch die Suchergebnisse navigieren. Wenn Sie in der Ergebnistabelle auf **Alle löschen** klicken, wird nur die Anzahl von Elementen gelöscht, die der maximalen Abfragegröße entspricht.

   Der Standardwert ist 1000.
4. Wählen Sie in der Liste **Zur Berichterstellung Metadaten speichern für** aus, wie viele Tage die Metadaten gespeichert werden und für die Generierung von Berichten zur Verfügung stehen sollen.

   Alle grafischen Berichte werden auf Grundlage des Parameters **Zur Berichterstellung Metadaten speichern für** erstellt.

   Der Standardwert ist **90 Tage**.

Konfigurieren der Server-Kommunikation mit McAfee Labs

Sie müssen SMTP-Server-Details angeben, damit MQM Daten und Elemente an McAfee Labs übermitteln kann. Dies ist der SMTP-Server, der E-Mails aus Ihrem Netzwerk sendet.

Beispielsweise wählen Administratoren Elemente aus, die von Benutzern als „Nicht-Spam" übermittelt wurden. MQM verwendet den SMTP-Server zum Einsenden von Elementen zur weiteren Analyse an McAfee Labs.

Vorgehensweise

1. Wählen Sie in MQM **Einstellungen und Diagnose** | **Erweiterte Einstellungen** aus.
2. Geben Sie im Feld **Port** die Port-Nummer ein, die der SMTP-Server für die Kommunikation mit McAfee Labs verwendet.

   Der Standardwert ist 25.

3 Geben Sie im Feld **IP-Adresse** die IP-Adresse des SMTP-Servers ein, der die Übermittlungen an McAfee Labs weiterleitet.

4 Geben Sie im Feld **Nachricht von** die E-Mail-Adresse der an McAfee Labs gesendeten E-Mail an.

Die Standard-E-Mail-Adresse des Absenders lautet McAfeeQuarantineManager@McAfee.dom.

Konfigurieren der Einstellungen für E-Mail-Benachrichtigungen

Sie können Absender- und Empfänger-E-Mail-Adressen für Benachrichtigungs-E-Mails von MQM angeben.

Benachrichtigungen können z. B. in folgenden Fällen erfolgen:

- Der MQM-Server stellt beim Ausfall der Datenbank den Betrieb ein.
- Aufgrund eines Server-Problems in der Cluster-Umgebung wird auf einen Standby-Server umgeschaltet.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Erweiterte Einstellungen** aus.

2 Geben Sie die E-Mail-Adresse des Absenders ein.

Die Standard-E-Mail-Adresse des Absenders lautet McAfeeQuarantineManager@McAfee.dom. Sie können diese E-Mail-Adresse ändern, damit sich die von MQM automatisch generierten E-Mails leichter erkennen lassen.

3 Geben Sie die E-Mail-Adresse des Empfängers ein.

Es empfiehlt sich, hier die E-Mail-Adresse des MQM-Administrators zu verwenden.

4 Passen Sie die für den E-Mail-Verkehr verwendete MQM-URL an.

- **Server-Name**: Die IP-Adresse bzw. der Domänenname verweist auf den Server, auf dem MQM installiert ist.

  Beispiel: domain.dom. Wenn die MQM-Website auf einem benutzerdefinierten Port ausgeführt wird, geben Sie den Pfad als „domain.dom:port-nummer" an.

- **Protokoll**: Wählen Sie HTTP oder HTTPS aus, um anzugeben, ob für den Domänenzugriff eine sichere Verbindung erforderlich ist. Das Protokoll richtet sich nach den Konfigurationseinstellungen des Servers, auf dem Microsoft Internetinformationsdienste ausgeführt werden.

- **Beispiel eines URLs für die Benutzeroberfläche für Anwender**: Vorschau eines Beispiels für eine benutzerdefinierte URL auf der Grundlage der ausgewählten Optionen.

  Beispiel: https://domain.dom/MQMUserUI. Der Domänenname lautet domain.dom, und es wird das Protokoll HTTPS verwendet.

Konfigurieren verschiedener Einstellungen

Konfigurieren Sie die Parameter für verschiedene Einstellungen.

Die Registerkarte **Einstellungen** steht nur Super-Administratoren und Operatoren zur Verfügung. Wenn Sie sich als Domänenadministrator anmelden, wird diese Registerkarte nicht angezeigt.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Erweiterte Einstellungen** aus.

2 Geben Sie in **Sitzungszeitlimit der Benutzeroberfläche für Administratoren (in Sekunden)** an, wie viele Sekunden sich die Benutzeroberfläche für Administratoren im Leerlauf befinden darf, bevor die Sitzung automatisch beendet wird.

Der Standardwert ist 600.

3 Geben Sie in **Sitzungszeitlimit der Benutzeroberfläche für Anwender (in Sekunden)** an, wie viele Sekunden sich die Benutzeroberfläche für Anwender im Leerlauf befinden darf, bevor die Sitzung automatisch beendet wird.

   Der Standardwert ist 600.

4 Geben Sie im Feld **Intervall für Dashboard-Aktualisierung (in Sekunden)** das gewünschte Aktualisierungsintervall für die Dashboard-Zähler ein.

   Der Standardwert ist 60.

Konfigurieren der Einstellungen für Statusbericht-E-Mails

Sie können die Status-E-Mail vor dem Senden an Administratoren in der Vorschau anzeigen, bearbeiten und anpassen.

Vorgehensweise

1 Wählen Sie in MQM **Einstellungen und Diagnose** | **Erweiterte Einstellungen** aus.

2 Geben Sie die für den Status-E-Mail-Bericht erforderlichen Informationen ein.

   a Geben Sie im Feld **E-Mail-Adresse des Absenders** die E-Mail-Adresse des Absenders ein.

   b Geben Sie im Feld **E-Mail-Adresse des Empfängers** die E-Mail-Adresse des Empfängers ein.

   c Geben Sie im Feld **Betreff** den Betreff der E-Mail ein.

Daraufhin öffnet sich ein Fenster, das den E-Mail-Inhalt als HTML-Code enthält. Sie können den Inhalt der E-Mail nun bearbeiten. Wenn ein bestimmtes Token nicht in der E-Mail enthalten sein soll, suchen Sie nach dem Tag, der dieses Token enthält, und löschen Sie ihn. Wenn die E-Mail beispielsweise keine Zählerinformationen enthalten soll, löschen Sie „%COUNTER_LIST%“.

Gleichzeitiges Freigeben mehrerer E-Mails

Sie können Parameter für die Massenfreigabe von E-Mails festlegen. Es können mehr als 100 E-Mails auf einmal freigegeben werden.

Vorgehensweise

1 Klicken Sie in der Benutzeroberfläche für Administratoren auf **Einstellungen und Diagnose** | **Kommunikation** | **Erweiterte Einstellungen** | **Auf McAfee-Produkte bezogene Vorgänge** (Systemlisten | SSO-Katalog).

2 Verwenden Sie für die Suche nach E-Mails, die Sie auf einmal freigeben möchten, einen einzelnen Suchfilter oder eine Kombination von mehreren Filtern.

3 Wählen Sie **Alle Daten** aus, oder wählen Sie **Datumsbereich** aus, und geben Sie einen Datumsbereich an.

4 Wählen Sie in der Dropdown-Liste **Domäne** die Domäne aus.

5 Klicken Sie für die Freigabe von mehreren Elementen auf **Freigeben**.

6 Klicken Sie zum Löschen aller ausgewählten Filter auf **Filter löschen**.

Siehe auch

Suchen nach isolierten Elementen auf Seite 59

Neuzuweisen von aus der Quarantäne freigegebenen E-Mails zu anderen Produkten

Sie können isolierte E-Mails eines McAfee-Produkts durch ein anderes Produkt freigeben. MQM gibt eine E-Mail über das McAfee-Produkt frei, das die E-Mail isoliert hat.

Sie können aus der Quarantäne freigegebene E-Mails einem anderen Produkt zuweisen, wenn das ursprüngliche McAfee-Produkt nicht verfügbar ist oder ein Upgrade für dieses Produkt durchgeführt wird.

Nur Super-Administratoren und Operatoren können McAfee-Produkt-IDs neu zuweisen. Wenn Sie sich als Domänenadministrator anmelden, wird diese Option nicht angezeigt.

Vorgehensweise

1. Klicken Sie in MQM auf **Einstellungen und Diagnose** | **Erweiterte Einstellungen** | **Auf McAfee-Produkte bezogene Vorgänge** für diese Domäne konfiguriert wurde.
2. Wählen Sie im Bildschirm **Erweiterte Einstellungen** die Option **Neuzuweisung eines McAfee-Produkts aktivieren** aus.
3. Geben Sie im Feld **Alte McAfee-Produkt-ID** die McAfee-Produkt-ID des Produkts ein, das die Elemente isoliert hat.
4. Geben Sie im Feld **Neue McAfee-Produkt-ID** die McAfee-Produkt-ID des Produkts ein, das die Freigabe durchführt.
5. Klicken Sie zum Speichern auf **Neu zuweisen**.

Die E-Mails werden an das neu zugewiesene McAfee-Produkt gesendet.

Konfigurieren von Zertifikaten für die sichere SMTP-Kommunikation

Sie können Zertifikate für die sichere (TLS) SMTP-Kommunikation konfigurieren.

Für die Installation auf dem SMTP-Server muss für die TLS-Kommunikation (Transport Layer Security) ein gültiges, von einer zugelassenen Zertifizierungsstelle ausgestelltes Zertifikat vorhanden sein. Das CA-Zertifikat muss auf dem McAfee Quarantine Manager-Server installiert sein, wenn die Option „TLS" für das Senden von E-Mails aktiviert wird.

Vergewissern Sie sich, dass das Zertifikat im PEM-Format vorliegt.

Vorgehensweise

1. Navigieren Sie im McAfee Quarantine Manager-Installationsverzeichnis zu \bin\certs.
2. Erstellen Sie eine Datei, und geben Sie ihr den Namen ca.pem.
3. Öffnen Sie die CA-Zertifikatsdatei, und kopieren Sie den Inhalt dieser Datei in die Datei ca.pem.

Wenn Sie über Zertifikate von unterschiedlichen Zertifizierungsstellen verfügen, kopieren Sie die Inhalte aller CA-Zertifikate in die Datei ca.pem.

Sichern der Datenbank

Im Falle eines Datenverlusts können Sie McAfee Quarantine Manager anhand einer Sicherung der vorhandenen Datenbank wiederherstellen.

Bei der Datenbanksicherung werden die folgenden Einstellungen gespeichert.

Tabelle 13-1 Einstellungen für die Datenbanksicherung

Einstellung	Beschreibung
McAfee Quarantine Manager-Benutzerkonto	Speichert Benutzerinformationen und E-Mail-Aliasse.
Blacklists und Whitelists	Speichert die von den Administratoren verwalteten globalen Blacklists und Whitelists.
Dashboards	Speichert Dashboard-Daten zum Bericht, zum McAfee Quarantine Manager-Server und zu den isolierten Elementen.
Isolierte Daten	Speichert die von McAfee Quarantine Manager in der Datenbank gespeicherten isolierten Daten.

Aufgaben

- *Sichern der Microsoft SQL Server-Datenbank* auf Seite 87
  Sie können die in Microsoft SQL Server gespeicherte McAfee Quarantine Manager-Datenbank sichern.
- *Wiederherstellen der Microsoft SQL Server-Datenbank* auf Seite 88
  Nach einem Datenverlust können Sie die McAfee Quarantine Manager-Datenbank aus einer Microsoft SQL Server-Datenbanksicherung wiederherstellen.
- *Sichern der MySQL-Datenbank* auf Seite 88
  Sichern Sie Ihre bestehende MySQL-Datenbank, die zum Lieferumfang von McAfee Quarantine Manager gehört.
- *Wiederherstellen der MySQL-Datenbank* auf Seite 88
  Nach einem Datenverlust können Sie eine gesicherte MySQL-Datenbank wiederherstellen.
- *Konfigurieren eines geplanten Sicherungs-Tasks für die MySQL-Datenbank* auf Seite 89
  Sie können eine Sicherung Ihrer MySQL-Datenbank planen, die zum Lieferumfang von McAfee Quarantine Manager gehört.

Sichern der Microsoft SQL Server-Datenbank

Sie können die in Microsoft SQL Server gespeicherte McAfee Quarantine Manager-Datenbank sichern.

Vorgehensweise

1 Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

2 Beenden Sie im Fenster **Dienste** den McAfee Quarantine Manager-Dienst.

3 Melden Sie sich bei Microsoft SQL Server Management Studio an.

4 Navigieren Sie durch die Datenbanken, und wählen Sie die McAfee Quarantine Manager-Datenbank aus.

5 Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Tasks** | **Sichern** aus.

6 Konfigurieren Sie die Einstellungen auf der Seite **Datenbank sichern**.

   a Wählen Sie in der Dropdown-Liste **Sicherungstyp** die Option **Vollständig** aus.

   b Wählen Sie in der Dropdown-Liste **Sicherungskomponente** die Option **Datenbank** aus.

   c Wählen Sie in der Dropdown-Liste **Sicherungssatz läuft ab** die Option **Nach** | **0** aus.

   d Wählen Sie unter **Ziel** die Option **Festplatte** aus.

e Wenn Sie den Standardspeicherort für die Sicherung ändern möchten, klicken Sie auf **Hinzufügen**, und navigieren Sie dann zum gewünschten Speicherort.

f Klicken Sie zum Speichern der Sicherungsdatei auf **OK**.

Wiederherstellen der Microsoft SQL Server-Datenbank

Nach einem Datenverlust können Sie die McAfee Quarantine Manager-Datenbank aus einer Microsoft SQL Server-Datenbanksicherung wiederherstellen.

Vorgehensweise

1 Kopieren Sie die Sicherungsdatei in das Zielsystem.

2 Melden Sie sich auf dem Zielsystem bei Microsoft SQL Server Management Studio an.

3 Erstellen Sie eine Datenbank, und wählen Sie sie dann aus.

4 Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie **Tasks** | **Wiederherstellen** aus.

5 Konfigurieren Sie die Einstellungen auf der Seite **Datenbank wiederherstellen**.

a Wählen Sie in der Dropdown-Liste **In Datenbank** die Datenbank aus.

b Wählen Sie in der Dropdown-Liste **Quelle für die Wiederherstellung** die Option **Von Medium** aus, und navigieren Sie zu der Sicherungsdatei (.bak), die wiederhergestellt werden soll.

Sichern der MySQL-Datenbank

Sichern Sie Ihre bestehende MySQL-Datenbank, die zum Lieferumfang von McAfee Quarantine Manager gehört.

Vorgehensweise

1 Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

2 Beenden Sie im Fenster „Dienste" den McAfee Quarantine Manager-Dienst.

3 Wechseln Sie an der Eingabeaufforderung zum bin-Verzeichnis des MySQL-Installationsordners.

4 Führen Sie den folgenden Befehl aus:

```
mysqldump --complete-insert -n --add-drop-table -R <Datenbank> -u
<Datenbankbenutzer> -p<Datenbankbenutzerkennwort> -r
"<VollständigerPfadSicherungsdatei>" --max-allowed-packet=1024M
```

Wenn beispielsweise der Datenbankname „mqm", der Benutzername „root", das Kennwort „dbase" und der Sicherungsspeicherort „C:\Backups\MQM\MQMBackup.sql" lauten, müssten Sie folgenden Befehl verwenden:

```
mysqldump --complete-insert -n --add-drop-table -R mqm -u root -pdbase -r "C:
\Backups\MQM\MQMBackup.sql" --max-allowed-packet=1024M
```

Wiederherstellen der MySQL-Datenbank

Nach einem Datenverlust können Sie eine gesicherte MySQL-Datenbank wiederherstellen.

Vorgehensweise

1 Klicken Sie auf **Start** | **Ausführen**, geben Sie `services.msc` ein, und klicken Sie dann auf **OK**.

2 Beenden Sie im Fenster **Dienste** den McAfee Quarantine Manager-Dienst.

3 Wechseln Sie an der Eingabeaufforderung zum bin-Verzeichnis des MySQL-Installationsordners.

4 Führen Sie den folgenden Befehl aus: `mysql -e "source <VollständigerPfadderSicherungsdatei>" -u <Datenbankbenutzer> -p<Datenbankbenutzerkennwort> <Datenbank>`

Wenn beispielsweise der Datenbankname „mqmv7", der Benutzername „root", das Kennwort „dbase" und der Sicherungsspeicherort „C:\Backups\MQM\MQMBackup.sql" lauten, müssten Sie folgenden Befehl verwenden: `mysql -e "source C:\Backups\MQM\MQMBackup.sql" -u root -pdbase mqmv7`

Konfigurieren eines geplanten Sicherungs-Tasks für die MySQL-Datenbank

Sie können eine Sicherung Ihrer MySQL-Datenbank planen, die zum Lieferumfang von McAfee Quarantine Manager gehört.

Vorgehensweise

1 Erstellen Sie eine Stapelverarbeitungsdatei mit folgenden Informationen:

```
md c:\backups\%DATE%\

cd c:\backups\%DATE%\

<Installationspfad>\bin\mysqldump.exe --complete-insert -n --add-drop-table -R <Datenbankname> -u <Benutzername> -p<Kennwort> -r "MQMBackup.sql"
```

2 Wählen Sie **Start** | **Systemsteuerung** | **Geplante Aufgaben** | **Geplante Aufgabe hinzufügen** aus.

3 Klicken Sie auf **Weiter**, und navigieren Sie zur Stapeldatei.

4 Klicken Sie auf **Weiter**.

5 Befolgen Sie die auf dem Bildschirm angezeigten Anweisungen, um den Task zu planen und den Assistenten abzuschließen.

14 Verwaltung von Blacklists und Whitelists

Die Blacklist ist eine Liste der E-Mail-Adressen, von denen Sie keine Spam- oder unerwünschten E-Mails empfangen möchten.

In der Whitelist werden die E-Mail-Adressen vertrauenswürdiger Quellen, beispielsweise von Geschäftspartnern, gespeichert, deren Nachrichten Sie empfangen möchten.

E-Mail-Adressen, die in Black- oder Whitelists eingetragen werden, werden in regelmäßigen Abständen mithilfe von Push an die verbundenen McAfee-Produkte übertragen. Hier können Sie Verwaltungsaktionen für die Black- und Whitelists durchführen, z. B. E-Mail-Adressen hinzufügen und löschen.

Inhalt

- *Blacklist- und Whitelist-Ebenen*
- *Konfigurieren des Konfigurationsübertragungsintervalls*
- *Verwalten von Blacklists und Whitelists*
- *Importieren von Blacklists und Whitelists*
- *Exportieren von Blacklists und Whitelists*

Blacklist- und Whitelist-Ebenen

Eine Blacklist ist eine Liste der E-Mail-Adressen, von denen der Benutzer keine E-Mails empfangen will. Die in der Whitelist aufgeführten E-Mail-Adressen werden vom Benutzer hingegen als Absender akzeptiert.

Mit McAfee Quarantine Manager können Benutzer persönliche Blacklists erstellen, die sie zusätzlich zu den vom Administrator verwalteten globalen Blacklists oder Blacklists für Gruppen verwenden. Nachrichten von Adressen, die in der Blacklist enthalten sind, werden blockiert oder isoliert. An die Benutzer gesendete E-Mails werden mit den Blacklists abgeglichen. Wenn die Absenderadresse mit einem der Einträge übereinstimmt, wird die entsprechende E-Mail nicht an den Benutzer übermittelt.

Mit McAfee Quarantine Manager können Benutzer persönliche Whitelists erstellen, die zusätzlich zu den vom Administrator verwalteten globalen Whitelists oder Whitelists für Gruppen verwendet werden. Nachrichten von Adressen, die in der Whitelist enthalten sind, gelten automatisch als legitime Nachrichten und werden niemals als Spam behandelt. An die Benutzer gesendete E-Mails werden mit den Whitelists abgeglichen. Wenn die Absenderadresse mit einem der Einträge übereinstimmt, wird die entsprechende E-Mail an den Benutzer übermittelt. Nachrichten von E-Mail-Adressen in der Whitelist werden nicht auf Phishing oder Spam, jedoch auf andere Aspekte hin gescannt.

In McAfee Quarantine Manager gibt es für Blacklists und Whitelists die folgenden drei Ebenen:

- **Global**: Diese Blacklists bzw. Whitelists werden für das gesamte Unternehmen zentral verwaltet.
- **Gruppe**: Diese Blacklists bzw. Whitelists werden für jede in verbundenen McAfee-Produkten definierte Benutzergruppe separat verwaltet.
- **Benutzer**: Diese Blacklists bzw. Whitelists werden für einzelne Benutzer verwaltet.

Sie können Blacklists und Whitelists auch Produkten, die mit McAfee Quarantine Manager verbunden sind, oder Benutzersätzen hinzufügen.

Konfigurieren des Konfigurationsübertragungsintervalls

Die Konfigurationsänderungen werden mithilfe von Push an die mit McAfee Quarantine Manager verbundenen Produkte übertragen.

Die Konfigurationsübertragung erfolgt in regelmäßigen Abständen. Sie können den Mindestabstand zwischen den Aktualisierungen der Konfiguration auf den verbundenen McAfee-Produkten angeben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Benutzeroberfläche für Administratoren auf **Einstellungen und Diagnose** | **Kommunikation** | **Erweitert** (Systemlisten | SSO-Katalog).
2. Geben Sie im Feld **Konfigurationsübertragungsintervall (in Sekunden)** das gewünschte Intervall ein.

   Der Standardwert ist 14400.

Verwalten von Blacklists und Whitelists

Sie können die Blacklists und Whitelists der Benutzer anzeigen und bearbeiten.

Sie können auch Benutzergruppen als E-Mail-Listen oder als Verweise auf vorhandene Benutzergruppen definieren.

E-Mail-Adressen, die Black- oder Whitelists hinzugefügt werden, werden regelmäßig mithilfe von Push an die verbundenen McAfee-Produkte übertragen.

Vorgehensweise

1. Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Blacklists und Whitelists** | **Organisation** (Systemlisten | SSO-Katalog).
2. Sie können die Blacklists verwalten.
   a. Klicken Sie auf die Registerkarte **Blacklists**.
   b. Geben Sie im Feld **Eintrag** die Blacklist-E-Mail-Adresse ein.
   c. Wählen Sie in der Dropdown-Liste **Listentyp** den Typ der gesuchten E-Mail-Adressliste aus, und klicken Sie dann auf **Suchen**.

Globale Blacklists können ausschließlich von Super-Administratoren und Operatoren geändert werden. Domänenadministratoren sind lediglich zum Anzeigen von globalen Blacklists berechtigt. Wenn Sie Gruppen-Blacklists Adressen hinzufügen, werden diese Adressen auch den Gruppen-Blacklists der verbundenen McAfee-Produkte hinzugefügt.

d Wenn Sie die Anzahl der pro Seite angezeigten Einträge ändern möchten, wählen Sie in der Dropdown-Liste **pro Seite** die gewünschte Option aus.

Standardmäßig werden pro Seite 20 Elemente angezeigt.

e Durch Klicken auf die Pfeile können Sie durch die Seiten blättern.

f Wenn Sie die E-Mail-Adresse der Blacklist hinzufügen möchten, klicken Sie auf **Hinzufügen**.

g Wenn Sie nach der E-Mail-Adresse suchen möchten, klicken Sie auf **Suchen**.

Für die Suche bzw. beim Hinzufügen von mehreren E-Mail-Adressen können Platzhalterzeichen verwendet werden.

- **?**: Entspricht einem einzelnen Zeichen.
- *****: Entspricht mehreren Zeichen.

Platzhalterzeichen können nur für Benutzer-IDs, nicht jedoch für Domänen verwendet werden. Beispiel:

- Wenn Sie alle E-Mail-Adressen von der Domäne abc.com hinzufügen möchten, die mit ka beginnen, geben Sie ka*@abc.com ein.
- Möchten Sie all Absender der Domäne abc.com hinzufügen, geben Sie *@abc.com ein.

h Wenn Sie alle Suchparameter löschen möchten, klicken Sie auf **Filter löschen**.

i Wenn Sie die ausgewählten E-Mail-Adressen entfernen möchten, klicken Sie auf **Löschen**.

j Wenn Sie alle E-Mail-Adressen entfernen möchten, klicken Sie auf **Alle löschen**.

3 Sie können die Whitelists verwalten.

a Klicken Sie auf **Whitelists**.

b Auf der Registerkarte **Whitelists** befinden sich die gleichen Optionen wie auf der Registerkarte **Blacklists**.

Importieren von Blacklists und Whitelists

Um Blacklists und Whitelists in McAfee Quarantine Manager verwenden zu können, müssen Sie sie zunächst importieren.

Sie können auch die globale Blacklist und Whitelist importieren.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Blacklists und Whitelists** | **Importieren und exportieren** (Systemlisten | SSO-Katalog).

2 Klicken Sie unter **Importieren** auf **Durchsuchen**, und navigieren Sie zur Blacklist oder Whitelist.

3 Klicken Sie auf **Konfiguration importieren**.

McAfee Quarantine Manager erkennt automatisch den Typ der Importdatei und aktualisiert die Datenbank.

4 Wählen Sie zum Zusammenführen der neuen Benutzerkonfiguration mit der früheren Benutzerkonfiguration die Option **Benutzerkonfiguration zusammenführen** aus.

Wenn die Option **Benutzerkonfiguration zusammenführen** nicht ausgewählt wird, wird die frühere Benutzerkonfiguration überschrieben. Mit der Option **Benutzerkonfiguration zusammenführen** können Sie auch Aliasse zusammenführen und Benutzer neu zuweisen.

Exportieren von Blacklists und Whitelists

Sie können Benutzerkonfigurationen, Blacklists und Whitelists für Gruppen sowie globale Blacklists und Whitelists exportieren.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Blacklists und Whitelists** | **Importieren und exportieren** (Systemlisten | SSO-Katalog).

2 Wählen Sie aus der Dropdown-Liste **Exporttyp** eine Option aus.

Wählen Sie bei Auswahl von **Benutzerkonfiguration** die Domänen aus der Dropdown-Liste **Domänen auswählen** aus. Wählen Sie bei Auswahl von **Gruppen-Black-/Whitelist** die Domänen aus der Dropdown-Liste **Gruppen** aus.

3 Klicken Sie auf **Konfiguration exportieren**.

Daraufhin öffnet sich das Fenster **Datei-Download**. Die Benutzerkonfiguration wird als XML-Datei exportiert.

4 Klicken Sie auf **Speichern**.

Der Standarddateiname lautet McAfeeBWList.xml.

Blacklists und Whitelists für Gruppen sowie globale Blacklists und Whitelists werden auf die gleiche Weise exportiert.

15 Dashboard und grafische Berichte

Die Benutzeroberfläche bietet wichtige Funktionen für McAfee Quarantine Manager-Administratoren. Administratoren müssen genau wissen, wie gut die Server gegen Spam- und Phishing-E-Mails, Viren, potenziell unerwünschte Programme und unerwünschte Inhalte geschützt sind. Das Dashboard ist Ihre Schnittstelle zum McAfee Quarantine Manager.

Inhalt

- *Anzeigen von Dashboard-Zählern*
- *Testen von verbundenen McAfee-Produkten*
- *Durchführen einer Schnellsuche*
- *Berechnen der Datenbankgröße*
- *Erstellen von mehrdimensionalen Berichten*
- *Erstellen von Top-10-Berichten*
- *Erstellen von spezifischen grafischen Berichten*
- *Herunterladen eines Berichts*

Anzeigen von Dashboard-Zählern

Das Dashboard bietet einen allgemeinen Überblick über den McAfee Quarantine Manager-Server, die isolierten Elemente und die Berichte.

Vorgehensweise

1. Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard** | **Grafische Berichte** | **Isoliert** (Systemlisten | SSO-Katalog).
2. Konfigurieren Sie die verfügbaren Optionen.

Testen von verbundenen McAfee-Produkten

Sie können alle mit McAfee Quarantine Manager verbundenen Produkte anzeigen und testen.

Vorgehensweise

1. Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard**.
2. Klicken Sie auf **Verbundene McAfee-Produkte**, und wählen Sie dann das gewünschte Produkt aus.
3. Klicken Sie auf **Testen**.

Die Funktion **Testen** unterstützt keine HTTP-basierten McAfee-Produkte.

Durchführen einer Schnellsuche

Mit der Schnellsuche können Sie nach einem isolierten Element suchen, ohne durch die Seite **Isolierte Objekte** navigieren zu müssen.

Vorgehensweise

1. Klicken Sie im Hauptmenü von **McAfee Quarantine Manager** auf **Dashboard**.
2. Klicken Sie auf die Registerkarte **Schnellsuche**.
3. Konfigurieren Sie die Optionen für den **Zeitraum**.
4. Wählen Sie in der Dropdown-Liste **Domäne** die Domäne aus.

   Wählen Sie zur Auswahl von Domänen, die nicht vom McAfee Quarantine Manager-Server verwaltet werden, **Andere** aus.
5. Geben Sie im Feld **Absender** die E-Mail-Adressen der Absender ein.
6. Geben Sie im Feld **Empfänger** die E-Mail-Adressen der Empfänger ein.
7. Geben Sie im Feld **Betreff** den Betreff der E-Mail ein.
8. Klicken Sie auf **Suchen**.
9. Klicken Sie zum Anzeigen der Ergebnisse auf **Quarantäne-Management** | **Isolierte Elemente** (Systemlisten | SSO-Katalog).

Siehe auch

Verwalten isolierter Elemente auf Seite 4

Berechnen der Datenbankgröße

Sie können die Größe der Datenbank und die Menge des verfügbaren Speicherplatzes auf der Festplatte abrufen.

Vorgehensweise

1. Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard**.
2. Klicken Sie auf die Registerkarte **Datenbankinformationen**.
3. Klicken Sie zum Abrufen der aktuellen Daten zur Datenbankgröße und Speicherplatznutzung auf **Datenbankgröße abrufen**. Wenn die Datenbank sehr groß ist, kann das Abrufen der Daten etwas dauern.

Erstellen von mehrdimensionalen Berichten

Sie können grafische Berichte erstellen, die Statistikdaten in Form von Balkendiagrammen darstellen.

Vorgehensweise

1. Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard**.
2. Klicken Sie auf der Seite **Statistik** auf die Registerkarte **Berichte**.
3. Wählen Sie in der Dropdown-Liste **Domänen** die Domäne aus.
4. Konfigurieren Sie die Optionen für den **Zeitraum**.

5 Wählen Sie in der Dropdown-Liste **Abfrage von** die Abfrage aus.

6 Klicken Sie auf **Generieren**.

Erstellen von Top-10-Berichten

Sie können grafische Berichte zu Quarantäne-Aktivitäten erstellen.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard** | **Grafische Berichte** | **Standard** (Systemlisten | SSO-Katalog).

2 Wählen Sie in der Dropdown-Liste **Zeitraum** den Zeitraum aus.

3 Wählen Sie in der Dropdown-Liste **Typ** den Typ des isolierten Elements aus.

4 Wählen Sie in der Dropdown-Liste **Filter** den Filter aus.

5 Klicken Sie auf **Suchen**.

Erstellen von spezifischen grafischen Berichten

Sie können isolierte Elemente detailliert in einem Diagramm darstellen und mithilfe von Filtern nach Erkennungen suchen.

Vorgehensweise

1 Klicken Sie im Hauptmenü von McAfee Quarantine Manager auf **Dashboard** | **Grafische Berichte** | **Erweitert** (Systemlisten | SSO-Katalog).

2 Wählen Sie bis zu drei Filter aus.

   a Wählen Sie in der Dropdown-Liste die Bedingung aus, und geben Sie anschließend im zugehörigen Feld den entsprechenden Suchparameter ein.

   b Wenn zwei oder mehr Suchkriterien verwendet werden sollen, wählen Sie **Und** aus.

   c Wenn mindestens eine der angegebenen Regeln angewendet werden soll, wählen Sie **Oder** aus.

3 Legen Sie den Zeitraum fest.

   - Wenn Sie einen Bericht für den gesamten verfügbaren Zeitraum generieren möchten, wählen Sie **Alle Daten** aus.
   - Wenn ein Bericht für einen bestimmten Zeitraum erstellt werden soll, klicken Sie auf **Datumsbereich** und anschließend zum Auswählen des gewünschten Zeitraums auf .

4 Wählen Sie einen Diagrammtyp aus.

   - Wenn ein Balkendiagramm erstellt werden soll, klicken Sie auf **Balkendiagramm**.
   - Wenn ein Kreisdiagramm erstellt werden soll, klicken Sie auf **Kreisdiagramm**, wählen Sie die entsprechende Datenabfrage aus der Dropdown-Liste **Abfrage von** aus, und geben Sie dann im Feld **Maximale Ergebnisse** an, wie viele Ergebnisse höchstens angezeigt werden sollen.

5 Klicken Sie auf **Suchen**.

6 Wenn Sie alle Sucheinstellungen löschen möchten, klicken Sie auf **Filter löschen**.

Herunterladen eines Berichts

Sie können grafische Berichte als PDF- oder HTML-Dateien herunterladen und speichern.

Vorgehensweise

1 Wenn der grafische Bericht in das PDF-Format konvertiert werden soll, klicken Sie auf das PDF-Symbol.

   a Klicken Sie zum Anzeigen des Berichts als PDF-Datei auf **Öffnen**.

   b Klicken Sie auf **Speichern**, um den Bericht als PDF-Datei zu speichern.

2 Wenn der grafische Bericht in das HTML-Format konvertiert werden soll, klicken Sie auf das Internet Explorer-Symbol.

   a Klicken Sie zum Öffnen der ZIP-Datei auf **Öffnen**.

   b Klicken Sie auf **Speichern**, um den Bericht zu speichern.

A Häufig gestellte Fragen

Wo finde ich Informationen über die Auswirkungen eines Virus?

Siehe *McAfee Global Threat Intelligence-Technologie* unter http://www.mcafee.com/us/threat-center/technology/global-threat-intelligence-technology.aspx.

Wie nehme ich Kontakt mit dem technischen Support auf?

Nähere Informationen finden Sie unter https://support.mcafee.com.

Halten Sie bitte die folgenden Informationen bereit, wenn Sie sich an den technischen Support wenden:

- Hersteller und Modell des Computers, auf dem MQM installiert ist
- Betriebssystem und Version
- Ggf. zusätzlich installierte Hardware
- Verwendeter Web-Browser und Version
- Diagnosebericht zu dem Problem

Welche Bildschirmauflösung wird für MQM empfohlen?

MQM sollte mit einer Bildschirmauflösung von mindestens 1024 x 768 Pixel angezeigt werden.

Gibt es ein Tool für die Integration von MQM und Outlook?

Ja, das *McAfee Customer Submission Tool (MCST)*. Sie können es von der McAfee-Website herunterladen.

Wie stelle ich den Benutzerauthentifizierungsmodus für den LDAP-Server ein?

Klicken Sie auf **Endbenutzerverwaltung** | **Allgemein** | **Authentifizierung**, und wählen Sie dann **LDAP-Server-Konten** aus.

Welche Versionen von MQM können auf diese Version aktualisiert oder migriert werden?

Sie können von MQM 7.0.1 auf diese Version migrieren.

Wie lange dauert es, Daten aus einer MySQL-Datenbank in eine Microsoft SQL-Server-Datenbank zu konvertieren?

Die Konvertierung von 45 GB Daten dauert etwa eine Stunde.

Wann sollte ich Benutzer neu zuweisen?

Sie sollten Benutzer beispielsweise neu zuweisen, wenn ein Benutzer das Unternehmen verlässt oder das Benutzerkonto vom LDAP-Server gelöscht wird.

Wie optimiere oder verkleinere ich die MySQL-Datenbank?

1 Wechseln Sie an der Eingabeaufforderung zum bin-Verzeichnis des MySQL-Installationsordners.

2 Führen Sie den folgenden Befehl aus, um sich bei der MySQL-Datenbank anzumelden:

```
mysql --user=<Datenbank-Benutzername> --password=<Datenbankkennwort>
<Datenbankname>
```

Beispiel:

```
mysql --user=scott --password=tiger mqm
```

3 Führen Sie den folgenden Befehl zum Optimieren der Datenbank aus:

```
call pOptimize();
```

Nach dem Abschluss der Optimierung öffnet sich eine MySQL-Eingabeaufforderung.

4 Führen Sie den folgenden Befehl zum Schließen der MySQL-Datenbank aus:

```
quit
```

Wie passe ich meine MySQL-Datenbank an, um die Leistung von MQM zu verbessern?

1 Öffnen Sie im MySQL-Installationsordner die Datei „my.ini".

2 Ändern Sie die folgenden Parameter zu den angegebenen Werten:
Innodb_buffer_pool_size = 1G Innodb_Log_File_Size = 512M Innodb_Thread_Concurrency = 512

3 Starten Sie über die Dienstkonsole den Dienst **MySQL for McAfee Quarantine Manager** neu.

Wie passe ich meine Microsoft SQL Server 2005-Datenbank an, um die Leistung von MQM zu verbessern?

1 Öffnen Sie **SQL Server Management Studio**.

2 Klicken Sie mit der rechten Maustaste auf die Datenbank **mqm**, und wählen Sie **Properties** (Eigenschaften) aus.

3 Klicken Sie im linken Fensterbereich auf **Files** (Dateien), und bearbeiten Sie die folgenden Parameter auf der rechten Seite.
Initial size for Data file = (~30 GB)
Autogrowth for Data file = 1 GB
Initial size for log file = 1 GB
Autogrowth for Log file = 512 MB

4 Klicken Sie im linken Fensterbereich auf **Options** (Optionen), und ändern Sie auf der rechten Seite **Recovery model** (Wiederherstellungsmodell) in **Simple** (Einfach).

5 Klicken Sie mit der rechten Maustaste auf **Database Instance** (Datenbankinstanz), und wählen Sie **Properties** (Eigenschaften) aus.

6 Klicken Sie im linken Fensterbereich auf **Advanced** (Erweitert), und ändern Sie auf der rechten Seite **Network Packet Size** (Netzwerkpaketgröße) in `32767`.

7 Schließen Sie **SQL Server Management Studio**.

Ich erhalte noch immer E-Mails von einem Absender, der in der Blacklist enthalten ist. Warum?

MQM ermöglicht die Verwaltung von Blacklists und Whitelists, die von verbundenen McAfee-Produkten geändert und verwaltet werden. Das Blockieren einer E-Mail-Adresse ist in MQM jedoch nicht möglich. Anfragen für Einträge in die Blacklist oder Whitelist werden an die verbundenen McAfee-Produkte gesendet, die entsprechende Aktionen für das Blockieren bzw. Zulassen von E-Mails durchführen.

Ist MQM in andere Produkte, wie z. B. VirusScan Enterprise und die Desktop-Anti-Spyware-Software, integriert?

Nein, MQM unterstützt die Gateway-Produkte McAfee Email Gateway, McAfee Security for Microsoft Exchange und McAfee Security for Lotus Domino (Windows und Linux).

Für wie viele Benutzer ist MQM ausgelegt?

MQM unterstützt bis zu 200.000 Benutzer.

Welche Datenbankgröße wird von MQM maximal unterstützt?

McAfee Quarantine Manager unterstützt eine Datenbankgröße von bis zu 500 GB.

Können mehrere E-Mail-IDs für einen Benutzer in einer einzelnen Quarantäne-Ansicht zusammengefasst werden?

Ja, durch das Erstellen von E-Mail-Aliassen.

Wie häufig sollte ein MQM-E-Mail-Digest-Task ausgeführt werden?

Sie sollten mindestens einmal pro Woche einen E-Mail-Digest-Task ausführen.

Kann man in MQM den E-Mail-Text der E-Mails mit gesperrtem Inhalt sehen?

Ja, Sie können den Inhalt der E-Mails lesen, die unter **Gesperrter Inhalt** isoliert sind.

Kann der Super-Administrator einen Task für die von einem Domänenadministrator verwalteten Domänen planen?

Ja. Der Super-Administrator kann Tasks für jede Domäne planen, selbst wenn die Domäne von einem Domänenadministrator verwaltet wird.

Können in MQM Digests für nicht registrierte Benutzer gesendet werden?

Ja. MQM unterstützt das Senden von Digests auch für nicht registrierte Benutzer.

Kann ich ein erneutes Branding für die Benutzeroberfläche durchführen?

Ja.

Können wir, falls die Appliance-ID in McAfee Email and Web Security oder McAfee Email Gateway geändert wurde, E-Mails freigeben, die mit der alten Appliance-ID isoliert wurden?

Ja, Sie können mithilfe der Funktion **Produktneuzuweisung** eine neue McAfee-Produkt-ID zuweisen, um die isolierten E-Mails freizugeben.

Wie kann gepacktes MySQL in externes MySQL konvertiert werden?

Sichern Sie die vorhandenen Daten mithilfe der DB-Tools, und importieren Sie sie in das externe MySQL.

Welches sind die häufigsten Probleme bei der Verbindung von McAfee Security for Microsoft Exchange mit MQM?

Bei der Arbeit mit McAfee Security for Microsoft Exchange können folgende Probleme auftreten:

- McAfee Security for Microsoft Exchange stellt keine Verbindung mit MQM her.
- McAfee Security for Microsoft Exchange wird im MQM-Dashboard angezeigt, aber die Testverbindung schlägt fehl.
- Das Produktprotokoll enthält zu viele Bind- und Unbind-Einträge.

Problembehebung: Stellen Sie im McAfee Security for Microsoft Exchange-Feld den folgenden Registrierungsschlüssel ein:

```
HKLM\SOFTWARE\McAfee\<Produkt>\RPC\ThreatQuarantineManager_Connect_Timeout = 10000
```

`<Produkt>` steht hier für McAfee Security for Microsoft Exchange.

Wie gehe ich vor, wenn keine Verbindung mit MQM hergestellt wird?

Führen Sie die folgenden Schritte aus:

1 Überprüfen Sie, ob eine Firewall den Überwachungsport von MQM (standardmäßig Port 49500) blockiert. Das Ändern der Port-Nummer wird nicht empfohlen, in zwingenden Fällen können Sie sie jedoch über die Benutzeroberfläche für Administratoren ändern. Klicken Sie auf **Einstellungen und Diagnose** | **Kommunikation** für diese Domäne konfiguriert wurde.

Vergewissern Sie sich, dass in den verbundenen McAfee-Produkten die gleiche Port-Nummer verwendet wird.

2 Überprüfen Sie den Überwachungsport in den verbundenen McAfee-Produkten.

- Für die McAfee Email and Web Security- und McAfee Email Gateway-Appliances wird der Überwachungsport in der Datei /etc/McAfee/TQMClient/SAFe.ini im Abschnitt `[TQMCallback]` angegeben.

  ```
  [TQMCallback]

  Port=#49500
  ```

- Für die McAfee Security for Microsoft Exchange-Appliances wird der Überwachungsport im folgenden Registrierungsschlüssel angegeben.

  ```
  HKLM\SOFTWARE\McAfee\<Produkt>\TQMCallback\Port = 49500
  ```

3 Starten Sie die MQM-Dienste neu, und achten Sie auf die Thread-Anzahl des RPCServ.exe-Prozesses. Wenn die Thread-Anzahl nicht ungefähr 70 beträgt, könnte ein Problem in der MQM-Server-Anwendung vorliegen.

4 Wenn das Problem weiterhin besteht, starten Sie die McAfee-Produkt-Dienste neu.

Wie passe ich die Anwendungs-URL an?

Die in E-Mail-Benachrichtigungen, wie z. B. Digest-E-Mails und Kennworterinnerungen, verwendete MQM-URL enthält standardmäßig „http:" und den vollqualifizierten Domänennamen im Format http://<IhreDomäne>/MQMUserUI. Sie können diese URL über **Erweiterte Einstellungen** | **Einstellungen** | **Einstellungen für E-Mail-Benachrichtigungen** anpassen. Folgende Optionen stehen zur Auswahl:

- **Server-URL anpassen**: Wählen Sie diese Option aus, um die Anwendungs-URL anzupassen.
- **Server-Name**: Geben Sie die IP-Adresse oder den Domänennamen an, die auf den Server verweisen, auf dem MQM installiert ist. Beispiel: domain.dom. Wenn die MQM-Website auf einem benutzerdefinierten Port ausgeführt wird, geben Sie den Pfad als „domain.dom:port-nummer" an.
- **Protokoll**: Wählen Sie **HTTP** oder **HTTPS** aus, um festzulegen, ob eine gesicherte Verbindung für den Domänenzugriff benötigt wird. Dies hängt von der Konfiguration des Servers ab, auf dem die Microsoft-Internetinformationsdienste ausgeführt werden.
- **Beispiel eines URLs für die Benutzeroberfläche für Anwender**: Vorschau eines Beispiels für eine benutzerdefinierte URL auf der Grundlage der ausgewählten Optionen. Beispiel: https://domain.dom/MQMUserUI, wobei es sich bei „domain.com" um den Domänennamen handelt und als Protokoll „https" verwendet wird.

Siehe auch

Upgrade auf die aktuelle Version von MQM auf Seite 23
Ändern der Benutzerkonfiguration auf Seite 57
Erneutes Branding von McAfee Quarantine Manager auf Seite 6
Neuzuweisen von aus der Quarantäne freigegebenen E-Mails zu anderen Produkten auf Seite 86

B Erneutes Branding von McAfee Quarantine Manager

Mit dem Kit für erneutes Branding von McAfee Quarantine Manager können Sie verschiedene Benutzeroberflächenkomponenten der Administrator- und der Benutzeransicht von McAfee Quarantine Manager entsprechend dem Auftritt Ihres Unternehmens gestalten.

Inhalt

- *Übersicht*
- *Anpassen der McAfee Quarantine Manager-Software an das Erscheinungsbild Ihres Unternehmens*

Übersicht

Mit dem Kit für erneutes Branding von McAfee Quarantine Manager können Sie verschiedene Komponenten der Benutzeroberfläche mit eigenen Farben und Textelementen gestalten.

Folgende Komponenten können Sie ändern:

- Firmenlogo
- Farbe der Titelleiste
- Farbe der oberen Link-Leiste
- Firmenname und Produktname
- Farbe der Datentabelle

Anpassen der McAfee Quarantine Manager-Software an das Erscheinungsbild Ihres Unternehmens

Hier wird erläutert, wie Sie die McAfee Quarantine Manager-Benutzeroberfläche mit Ihrem Firmenlogo und den Unternehmensfarben und -slogans versehen sowie einige weitere Veränderungen vornehmen können.

Hinzufügen des eigenen Logos

Sie können das Erscheinungsbild der MQM-Benutzeroberfläche ändern, indem Sie Ihr eigenes Firmenlogo hinzufügen.

- Löschen Sie nicht die vorhandene Datei logo.gif.
- Platzieren Sie die Logodatei nicht außerhalb des MQM-Administrator-UI-Verzeichnisses. Geben Sie immer den relativen Pfad vom MQM-Administrator-UI-Ordner an.
- Sie können jedes Bildformat verwenden, das in einem Web-Browser dargestellt werden kann.
- Verwenden Sie für das Logo nur Bilder, die höchstens 1 MB groß sind.

Vorgehensweise

1. Passen Sie die Größe Ihres Firmenlogos an das Seitenverhältnis 3:1 an.
2. Öffnen Sie den Ordner **Rebrand** (<Installationsordner>\adminui\Rebrand.
3. Öffnen Sie die Datei Rebrand.js, und ändern Sie die folgende Zeile von LogoImagePath ../Rebrand.logo.gif in ../Rebrand/<Ihr_Logo>.gif

Verwenden der Unternehmensfarben

Sie können die obere Link-Leiste und die Titelleiste von MQM mit den Farben Ihres Unternehmens versehen.

Achten Sie darauf, einen gültigen Farbode zu verwenden, der vom Browser interpretiert werden kann. Ungültige Farbcodes können Skriptfehler auslösen und dazu führen, dass die Oberfläche nicht korrekt dargestellt wird.

Vorgehensweise

1. Öffnen Sie die Datei Rebrand.js, die sich im Installationsordner von MQM befindet.
2. Ändern Sie die Zeile `TitlebarColor = #B00C33 zu TitlebarColor = # 99CC33`, wobei `#99CC33` für den Farbcode der von Ihnen gewünschten Farbe steht.
3. Ändern Sie die Zeile `TopLinkBarColor = #000000` zu `TopLinkBarColor = #B00C33`, wobei `#B00C33` für den Farbcode der von Ihnen gewünschten Farbe steht.

Ändern des Firmen- und Produktnamens

Sie können Ihren Firmennamen auf der MQM-Benutzeroberfläche verwenden.

Damit die Titelleiste nicht verzerrt dargestellt wird, dürfen der Firmenname und der Produktname zusammen höchstens 100 Zeichen lang sein.

Vorgehensweise

1. Öffnen Sie im Ordner **Rebrand** im Installationsverzeichnis die Datei Rebrand.js.
2. Navigieren Sie zur Zeile `CompanyName = McAfee ProductName = Quarantine Manager`.
3. Ändern Sie den Firmennamen (CompanyName) in den Namen Ihrer Firma und den Produktnamen (ProductName) in `Speicher für isolierte E-Mails`.

Änderungen an der Darstellung der Oberfläche für Benutzer

Sie können das Erscheinungsbild der Benutzeroberfläche für die Benutzer ändern.

Vorgehensweise

1. Öffnen Sie den Ordner <MQM-Installationsordner>\userUI\Rebrand.
2. Nehmen Sie Änderungen an der Datei Rebrand.js vor:
   a. Öffnen Sie die Datei Rebrand.js.
   b. Nehmen Sie die erforderlichen Änderungen vor, und speichern Sie dann die Datei.

Index

A

Administrator
- Mit LDAP-Gruppen 44
- Typen 43

Administratoren, Benutzeroberfläche
- Erneutes Branding 105

Administratortyp
- Domänenadministrator 43
- Domänenadministrator-Alias 43
- Operator 43
- Super-Administrator 43
- Super-Administrator-Alias 43

Aliasse
- Hinzufügen 75

Ändern
- Domänenkonfigurationen 49
- Endbenutzerkonfiguration 57
- Kennwort 74
- Konfigurationseinstellungen 74

Anpassen
- Anwendungs-URL 99

Anwendungs-URL
- Anpassen 99

Anzeigen
- Produktprotokoll 79

Anzeigen von Suchergebnissen
- Übermittlungen durch Benutzer 66

Arbeitsspeicher 17

Aufruf zur Agentenreaktivierung
- Senden 33

Aufrufen
- Benutzeroberfläche 67

Authentifizierung
- Modi 44

B

Bearbeiten von Richtlinien
- ePolicy Orchestrator 32

Befehlszeilenargumente
- McAfee Quarantine Manager 29
- MySQL for McAfee Quarantine Manager 28

Benutzer
- Importieren 55

Benutzerdefinierte Warteschlangen 95

Benutzerinteraktionen 67

Benutzeroberfläche
- Aufrufen 67
- Erneutes Branding 99, 105, 106
- Farbe ändern 106
- Quarantäne verwalten 68

Benutzersynchronisierung 62

Benutzersynchronisierungs-Task
- Erstellen 62

Berechnen
- Datenbankgröße 96

Bereinigungs-Task
- Erstellen 62

Bereitstellung
- McAfee Agent 26
- McAfee Quarantine Manager 29
- MySQL for McAfee Quarantine Manager 28
- Paket und Erweiterung 26

Bericht
- Herunterladen 98

Berichte
- Generieren 97
- Konfigurieren 33
- Mehrdimensional 96

Berichtserweiterung
- Installieren 30

Betriebssysteme 17

Bildschirmauflösung
- Empfohlen 99

Blacklist
- Typen 91
- Verwalten 73
- Verwaltung 91

Blacklists
- Exportieren 94
- Importieren 93
- Verwalten 92

C

Cluster
- Konfiguration unter Windows 2003 21
- Konfiguration unter Windows 2008 22

Cluster *(Fortsetzung)*
Konfiguration unter Windows 2008 R2 22
Cluster-Installation 21

D

Dashboard 95
Dashboard-Zähler
Anzeigen 95
Datenbank
Feineinstellung 99
Konfigurieren 37
Optimieren 99
Datenbankeinstellungen
Konfigurieren 83
Datenbanken, unterstützte 17
Datenbankgröße
Berechnen 96
Datenbanksicherung
Erstellen 86
Datenträger
Gespeicherte Proben übermitteln 71
Datenverlust, Schutz 95
Debug-Verfolgung 80
Deinstallation 23
Deinstallieren 23
McAfee Quarantine Manager 23
MySQL for McAfee Quarantine Manager 23
Diagnose 80
Diagnoseeinstellungen
Konfigurieren 80
Digest-E-Mail 70
Digest-E-Mails
Quarantäne verwalten 70
Dokumentation
Produktspezifisch, suchen 8
Typografische Konventionen und Symbole 7
Zielgruppe dieses Handbuchs 7
Domäne
Exportieren 48
Hinzufügen, neu 48
Importieren 48
Verwalten 47
Domänen
Hinzufügen 47
Importieren 47
Domänenadministratoren
Domänen zuweisen 49
Domänenkonfigurationen
Ändern 49
Durchführen
Schnellsuche 96
Durchführen von Aktionen
Isolierte Elemente 59

E

E-Mail
Neuzuweisungen anzeigen 75
E-Mail-Benachrichtigungen
Konfigurieren 84
E-Mail-Digest-Task
Erstellen 61
Eigenes Konto
Verwalten 72
Einchecken des Pakets
McAfee Quarantine Manager 27
MySQL for McAfee Quarantine Manager 27
Einführung
McAfee Quarantine Manager 9
Eingeschränkte Berechtigungen
Administratoren erstellen mit 45
Endbenutzer
Automatisch registrieren 56
Erstellen 53
Importieren 55
Importieren aus Datei 54
Importieren über LDAP 53
Endbenutzerkonfiguration
Ändern 57
Entfernen
Erweiterungen 25
McAfee Quarantine Manager von Client-Computern 35
McAfee Quarantine Manager--Produkterweiterung 36
McAfee Quarantine Manager-Paket 35
MySQL for McAfee Quarantine Manager von Client-Computern 35
MySQL for McAfee Quarantine Manager-Paket 35
Software-Pakete 25
ePO
Siehe „McAfee ePO“ 26
ePolicy Orchestrator
Berichte konfigurieren 33
Deinstallieren der Software 34
Erweiterte Einstellungen 82
Festlegen von Richtlinien in 31
Installieren der Software mit 26
Integration 25
Richtlinien bearbeiten 32
Richtlinien erstellen 32
Richtlinien erzwingen 32
Voraussetzungen 25
Erfassen von Ausnahmen 80
Erneutes Branding 105
Benutzeroberfläche ändern 106
Benutzeroberfläche für Administratoren ändern 105
Eigenes Firmenlogo hinzufügen 105
Farbe ändern 106
McAfee Quarantine Manager 39
Verwenden des Firmennamens 106
Erste Schritte 9

Erstellen
Administratoren 45
Benutzersynchronisierungs-Task 62
Bereinigungs-Task 62
Datenbanksicherung 86
E-Mail-Digest-Task 61
Endbenutzer 53
Spezifische grafische Berichte 97
Status-E-Mail-Task 63
Zuordnung von Gruppen in verbundenen McAfee-Produkten zu einer Domäne 51
Erstellen von Richtlinien
ePolicy Orchestrator 32
Erweitert
Server-Einstellungen 82
Erweiterte Einstellungen
Datenbank 83
E-Mail-Benachrichtigungen 84
ePolicy Orchestrator 82
Statusbericht-E-Mail 85
Übermittlung an McAfee Labs 83
Verschiedenes 84
Erweiterung
Bereitstellung 26
Erzwingen von Richtlinien
ePolicy Orchestrator 32
Exportieren
Blacklists 94
Domäne 48
Whitelists 94

F

False-Negative 95
False-Positive 95
FAQs 99
Fehlerberichterstellung 80
Festlegen von Richtlinien in
ePolicy Orchestrator 31
Freigeben
Massen-E-Mails 85
Funktionen
Produkt 9

G

Grafische Berichte 95
Spezifisch 97
Größe des Thread-Pools 81
Gruppenzuordnung 51

H

Handbuch, Informationen 7
Häufig gestellte Fragen 99
Herunterladen
Bericht 98
Hilfeerweiterung
Installieren 31
Hinzufügen
Aliasse 75
Hochverfügbarkeit 21
Hochverfügbarkeit konfigurieren 12

I

Importieren
Blacklists 93
Domäne 48
Endbenutzer 53–55
Whitelists 93
Importieren von Benutzern
Aus Datei 54
Importieren von Endbenutzern
Über LDAP 53
Inhalt, Lieferumfang des Produkts 10
Installation
Berichtserweiterung 30
Cluster-Installation 21
Hilfeerweiterung 31
Richtlinienerweiterung 30
Übersicht über Tasks 18
Unterstützte McAfee-Produkte 11
Installieren
McAfee Quarantine Manager 21
MySQL for McAfee Quarantine Manager 19
Isolierte Elemente
Aktionen durchführen 59
Suchen 59
Verwalten 59
Isolierte Nachrichten
Beibehalten 70
Blacklist löschen 70
Freigeben 70
Löschen 70
Whitelist löschen 70

K

Kennwort
Ändern 74
Kommunikation
Konfigurieren 81
Komprimierungsprogramme 95
Konfigurationseinstellungen
Ändern 74
Konfigurationsübertragungsintervall 81
Konfigurieren
Berichte 33
Cluster 21, 22
Datenbank 37
Datenbankeinstellungen 83
Diagnose 80

Konfigurieren *(Fortsetzung)*
E-Mail-Benachrichtigungen 84
Erweiterte Einstellungen 82
Hochverfügbarkeit 12
Kommunikation 81
LDAP-Server 81
McAfee Email and Web Security Appliance 38
McAfee Security for Microsoft Exchange 38
MySQL 5.1 Linux 20
MySQL 5.1 Windows 20
Statusbericht-E-Mail 85
Übermittlung an McAfee Labs 83
Verschiedene Einstellungen 84
VMware-Unterstützung 13
Zertifikate 86
Konfigurieren der Datenbank
Microsoft SQL Server 19
Konfigurieren von Berichten
ePolicy Orchestrator 33
Konventionen und Symbole in diesem Handbuch 7

L

LDAP-Gruppen
Als Administrator fungieren 44
Als Administratoren 44
LDAP-Server
Konfigurieren 81
Logo
Firmenlogo hinzufügen 105

M

Massen-E-Mails
Freigeben 85
Maximale Kommunikationswiederholungen 81
McAfee Agent
Bereitstellen 26
McAfee Customer Submission Tool 99
McAfee Email and Web Security Appliance
Konfigurieren 38
McAfee ePO
Paket und Erweiterung bereitstellen 26
Verwalten von Quarantine Manager 12
McAfee Quarantine Manager
Auf Client-Computern bereitstellen 29
Befehlszeilenargumente 29
Deinstallieren 23
Einchecken des Pakets 27
Erneutes Branding 39
Installieren 21
Integrieren in ePolicy Orchestrator 25
Paket entfernen 35
Produkterweiterung entfernen 36
Testen 38
Upgrade 23
McAfee Quarantine Manager *(Fortsetzung)*
Von Client-Computern entfernen 35
McAfee Quarantine Manager, Einführung 9
McAfee Security for Microsoft Exchange
Konfigurieren 38
McAfee ServicePortal, Zugriff 8
Mehrdimensionale Berichte
Generieren 96
Mehrere E-Mail-IDs
Reduzieren 99
Microsoft Outlook
Proben übermitteln 71
Microsoft SQL Server
Datenbank konfigurieren 19
Microsoft SQL-Datenbank
Sichern 87
Wiederherstellen 88
Modi
Authentifizierung 44
MySQL 5.1
Linux, konfigurieren 20
Windows, konfigurieren 20
MySQL for McAfee Quarantine Manager
Auf Client-Computern bereitstellen 28
Befehlszeilenargumente 28
Deinstallation 23
Installieren 19
Paket einchecken 27
Paket entfernen 35
Von Client-Computern entfernen 35
MySQL-Datenbank
Sichern 88
Sicherung planen 89
Wiederherstellen 88

N

Neu zuweisen 86
Neuzuweisungsliste 86
Neuzuweisungsliste für McAfee-Produkte
Erstellen 86

O

Oberfläche
Erneutes Branding 105, 106
Farbe ändern 106
Objektübertragungsintervall 81
Operator
Administratortyp 43
Optimieren
Datenbank 99

P

Paket
    Bereitstellung 26
Phishing 95
Planen einer Sicherung
    Für MySQL-Datenbank 89
Potenziell unerwünschte Programme 95
Produkt
    Funktionen 9
Produktinhalt 10
Produktprotokoll 80
    Anzeigen 79
Protokollierung 80

Q

Quarantäne
    Proben übermitteln 72
Quarantine Manager
    Mit McAfee ePO 12

R

Reduzieren
    Mehrere E-Mail-IDs 99
Registrieren
    Endbenutzer, automatisch 56
    Verteilerliste 57
Richtlinienerweiterung
    Installieren 30

S

Schnellsuche
    Durchführen 96
Senden eines Aufrufs zur Agentenreaktivierung 33
Server-Einstellungen
    Erweitert 82
Server-Konfiguration
    Verwalten 79
Server-Verwaltung 43
ServicePortal, Quellen für Produktinformationen 8
Sichern der Datenbank
    Microsoft SQL 87
    MySQL 88
SMTP-Kommunikation 86
Spam 95
Spam-Proben
    Übermitteln 70
Spezifisch
    Grafische Berichte 97
Spezifische grafische Berichte
    Erstellen 97
Statistiken 95
Status-E-Mail 63
Status-E-Mail-Task
    Erstellen 63
Statusbericht-E-Mail
    Konfigurieren 85
Suchen
    Isolierte Elemente 59
Systemanforderungen 17
Szenarios
    VMware 13

T

Technischer Support 99
Technischer Support, Produktdokumentation finden 8
Testen
    McAfee Quarantine Manager 38
    Verbundene McAfee-Produkte 95
Top-10-Berichte 97
Transport Layer Security 86
Typen
    Administrator 43

U

Übermitteln von Proben 70
    Datenträger 71
    Microsoft Outlook 71
    Quarantäne 72
Übermittlung an McAfee Labs
    Konfigurieren 83
Übermittlungen durch Benutzer 65
    Suchergebnisse anzeigen 66
    Verwalten 65
Übertragungsintervall
    Konfigurieren 92
Unerwünschter Inhalt 95
Unterstützte
    Betriebssysteme 17
    Browser 17
    Datenbanken 17
    McAfee-Produkte 11, 17
    Upgrades 17, 23
Upgrade
    Unterstützt 23
Upgrade auf
    McAfee Quarantine Manager 7.0 23
Upgrades, unterstützte 17

V

Verbundene McAfee-Produkte
    Testen 95
Vergrößern des Diagramms 95
Verschiedene Einstellungen
    Konfigurieren 84
Verschiedenes
    Erweiterte Einstellungen 84

Verschlüsselungs-Compliance 95
Verteilerliste
    Registrieren 57
Verwalten
    Blacklist 73, 91
    Blacklists 92
    Domänen 47
    Isolierte Elemente 59
    Quarantäne 68, 70
    Server-Konfiguration 79
    Übermittlungen durch Benutzer 65
    Whitelist 73, 91
    Whitelists 92
Verwaltungs-Software
    ePolicy Orchestrator 25
Viren 95
VMware
    Szenarios 13
VMware-Unterstützung
    Konfigurieren 13
Voraussetzungen
    Arbeitsspeicher 17
    ePolicy Orchestrator 25
    Netzwerk 17
    Speicherplatz 17
    System 17
Vorbereitung der Installation 19

W

Whitelist
    Typen 91
    Verwalten 73
    Verwaltung 91
Whitelists
    Exportieren 94
    Importieren 93
    Verwalten 92
Wiederherstellen der Datenbank
    Microsoft SQL 88
Wiederherstellen einer Datenbank
    MySQL 88
Windows-Komponenten, erforderliche 17

Z

Zähler 95
Zentrale Richtlinienverwaltung
    ePolicy Orchestrator 25
Zertifikate
    Konfigurieren 86
Zertifizierungsstelle 86
Zuweisen von Domänen
    Domänenadministratoren 49